EL AGENTE ENCUBIERTO INFORMÁTICO COMO TÉCNICA DE INVESTIGACIÓN ESPECIAL EN LA LEGISLACIÓN PENAL ECUATORIANA

GALO SEBASTÍAN MUÑOZ

31 DE MAYO DE 2023
PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
Quito

Capítulo I. Conceptualización del fenómeno del cibercrimen

1.1. Conceptualización de ciberdelincuencia y delitos informáticos

- **a)** Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos
- **b)** Delitos informáticos
- **c)** Delitos relacionados con el contenido

1.2. Ciberdelincuencia organizada y el fenómeno de la corporativización del cibercrimen.

1.3. Las redes anónimas y su relación con el cibercrimen

Capítulo II. Técnicas especiales de investigación: El agente encubierto informático

2.1. Concepto de técnicas especiales de investigación y agente encubierto informático

a) Aspectos delimitadores del agente provocador y el delito provocado

b) Ámbito de actuación del agente encubierto informático

c) Principios rectores del agente encubierto informático

2.2. Derecho comparado: El agente encubierto informático en la legislación española

Capítulo III. Efectos en los Derechos Humanos en la era digital: derecho a la intimidad personal y familiar y protección a los datos personales: autodeterminación informativa

3.1. Derecho a la privacidad e intimidad

3.2. Derecho a la protección de los datos personales en el marco de la investigación criminal: autodeterminación informativa.

Conclusiones

Recomendaciones

Referencias

Capítulo I.

1.1. Conceptualización de ciberdelincuencia y delitos informáticos

A partir del siglo XXI, la humanidad comienza una transición hacia una sociedad donde la difusión, uso, integración y manejo de información es relevante en los ámbitos económicos, políticos y culturales. Su principal impulsor es la información digital y las tecnológicas de la comunicación, esta gran cantidad de información está cambiando profundamente todos los aspectos sociales de la organización social, incluyendo la economía, la educación, la salud, las guerras, las formas de gobierno y la democracia. Las personas que cuentan con los medios para ser parte de esta sociedad de la información son llamados ciudadanos digitales. Esta es una de las etiquetas con las cuales se ha identificado a los humanos que están entrando en una nueva fase de la sociedad (Beniger, 1986).

En efecto, la influencia de las tecnologías de la información y comunicación en la sociedad trasciende de la mera estructura informática, ya que su presencia es esencial para el progreso social, debido a que fomenta la generación, disponibilidad y uso de las herramientas o servicios digitales. Por ejemplo, la sustitución del correo postal tradicional por el correo electrónico; los servicios de medicina se han adaptado ofreciendo la posibilidad a los usuarios de ser atendidos a través de medios telemáticos, y así en un sinfín de servicios que se han ajustado a las necesidades de la era digital.

Además, en los últimos datos de la Unión Internacional de Telecomunicaciones confirman que el uso de Internet se ha acelerado durante la pandemia. En 2019, el 54% de la población mundial, es decir, 4.100 millones de personas, utilizaban Internet. Desde entonces, el número de usuarios ha aumentado en 800 millones, alcanzando los 4.900 millones en 2021, lo que representa el 63%

de la población (UIT, 2021). Debido a este hecho, los usuarios de Internet están optando por tener más dispositivos móviles para realizar actividades como el comercio electrónico, transacciones financieras en línea y comunicación entre usuarios digitales. Sin embargo, la falta de conciencia sobre la ciberseguridad, especialmente entre grupos vulnerables como los ancianos, ha resultado en un aumento alarmante de las víctimas de ciberdelitos (INTERPOL, 2021).

La rápida expansión del uso de internet y la tecnología informática, combinada con la falta de conciencia sobre la seguridad en línea, ha creado una creciente oportunidad para la ciberdelincuencia. Actualmente, la informática, las redes y los datos pueden relacionarse con una amplia variedad de delitos. Además, la estructura digital de internet y la facilidad para adquirir la tecnología de la información y la comunicación han permitido que el cibercrimen se vincule con la delincuencia organizada y tenga un carácter transnacional. Como resultado, una de las principales consecuencias de la ciberdelincuencia es su capacidad de cometer actos ilícitos desde cualquier lugar del mundo y su dificultad para ser rastreada, lo que facilita que los delincuentes eviten ser capturados y castigados. También significa que cualquier persona puede ser víctima de cibercrimen, independientemente de su ubicación o experiencia en tecnología.

Así mismo, resulta complicado medir las consecuencias de los ciberdelitos en la sociedad, ya que resulta complejo calcular las pérdidas económicas provocadas por el cibercrimen como la cantidad de delitos denunciados, debido a que las víctimas no siempre informan de ello a las autoridades por falta de confianza en la administración de justicia o por la dinámica misma de los ciberdelitos. Según estimaciones del Registro de Direcciones de Internet de América Latina y el Caribe (2020), el costo anual del delito cibernético en América Latina se estima en $90 mil millones de dólares. Los países con más ataques en la región son Brasil y México, seguidos por

Colombia (21,73 por ciento), Argentina (13,94 por ciento), Perú y Ecuador, cada uno con 11,22 por ciento.

Esta forma de criminalidad informática se la considera como "delincuencia de cuello blanco" (Posada, 2017, p. 33), esto se debe a que los perpetradores de este tipo de delitos tienen el poder económico, intelectual y los medios necesarios para actuar de manera efectiva en el entorno digital, desde donde crean canales ilegales de acumulación de riqueza, estructuras de poder más o menos permanentes y abusan de su poder y de las instituciones para influir en el sistema político (Simonnetti, 2016).

Los ciberdelincuentes conocen sobre informática y sus componentes, además cuentan con la habilidad de comunicarse en distintos idiomas para participar en canales de comunicación a nivel global, lo que demuestra un cambio en la percepción colectiva acerca de los cibercriminales. Hace un tiempo atrás, se asociaba a un joven solitario en el sótano de su madre, pero esa idea ha sido desmentida y ahora se considera que son formas reales de crimen organizado.

Por lo tanto, para comprender el concepto de ciberdelincuencia, es importante señalar que no hay una definición universalmente aceptada y que tampoco define ni describe una categoría de delito claramente establecida. Esto se debe a la presencia constante de las computadoras y su versatilidad, así como a la evolución continua de las tecnologías de la información y la comunicación desde fines de la década de 1950 (Muñoz, 2021, p. 23). En los últimos años, el término "cibercrimen" ha comenzado a ser utilizado con mayor frecuencia por los expertos en informática (Lusthaus, 2018).

Sin embargo, existe una cierta similitud en los componentes esenciales de la definición de esta clase de delitos cibernéticos. Dependiendo del contexto, el término "ciberdelincuencia" puede

hacer referencia a crímenes cometidos a través de las TIC, a crímenes perpetrados contra las TIC y sus usuarios, o a supuestos actos ilícitos en los que las TIC desempeñan un papel secundario de ayuda. Por lo tanto, se puede definir la ciberdelincuencia como "(…) un acto que infringe la ley y que se comete usando las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, sitios web y tecnología o para facilitar un delito" (UNODC, 2020, p.34).

Al ser un tema poco abordado por la doctrina penal la definición de ciberdelincuencia se basa en la protección de bienes jurídicos. Esto incluye aquellos delitos que ponen en peligro o lesionan a la seguridad de la información, es decir, aquellas conductas que afecten a la disponibilidad, accesibilidad e integridad de los datos o sistemas informáticos. También incluye aquellos delitos relacionados con la computadora como el fraude y la falsificación informática, el contacto con fines sexuales con menores de edad, y aquellos delitos relacionados con el contenido, como la comercialización o tenencia de material de abuso sexual de niños, niñas y adolescentes. De acuerdo con Posada Maya (2017), estos delitos pueden afectar directamente bienes jurídicos tradicionales como el patrimonio, la fe pública, la intimidad personal y familiar, el honor, la indemnidad sexual de los menores.

En consecuencia, la complejidad radica en que varios de los tipos penales abiertos establecidos en el Código Orgánico Integral Penal podrían incluirse dentro de la categoría de delitos informáticos (Posada, 2017). De esa manera, la doctrina dominante en el tema ha considerado que:

> […] entre la manipulación de los sistemas informáticos, los datos y la información utilizados como medios concretos, y la afectación de los bienes jurídicos clásicos, debe existir una relación modal concreta desde la fase ejecutiva hasta el agotamiento del respectivo delito, cuando el último sea necesario. Esta razón modal comporta, por consiguiente, un mayor desvalor de acción objetivo en la realización de los delitos informáticos en sentido amplio o delitos vinculados a delitos comunes. (Posada, 2017, 102)

Es así como a la ciberdelincuencia se la ha clasificado en dos categorías distintas: delitos informáticos en sentido estricto y delitos informáticos en sentido amplio. Los delitos informáticos

en sentido estricto (o cibercrimen puro) es un término que se refiere a aquellas actividades delictivas que requieren necesariamente el uso de ordenadores, redes informáticas o tecnología de la información y comunicación. Sin estos componentes tecnológicos, el actor cibernético no podría cometer este tipo de delitos, que incluye la creación, difusión y comercialización de software malicioso, piratería para obtener información confidencial de organizaciones públicas y privadas (Muñoz, 2021, p. 23), ataques de denegación de servicios distribuidos (DDoS), y otros crímenes que ponen en peligro o lesionan de manera directa la confidencialidad, integridad de los sistemas y datos informáticos (EUROPOL, 2020).

Por otro lado, los delitos informáticos en sentido amplio (o delitos cometidos por humanos en los sistemas informáticos) se refieren a una amplia gama de delitos tradicionales que son facilitados por internet o los sistemas informáticos, como la distribución de material de abuso sexual de niños, niñas o adolescentes, la falsificación informática, fraudes informáticos.

Por lo tanto, los delitos informáticos en sentido amplio o delitos cometidos por humanos en los sistemas informáticos son aquellas "conductas punibles tradicionales de medios ejecutivos abiertos, que tienen una relación modal objetiva –aunque circunstancial– con el tratamiento de datos e información y los sistemas informáticos (utilización de elementos incorporales)" (Posada, 2017, p. 102). Estos delitos tienden a lesionar o poner en peligro bienes jurídicos clásicos como el honor, la libertad, la fe pública, el patrimonio económico y la formación sexual. Esta postura amplía el alcance de los delitos informáticos a los delitos tradicionales, al considerarlos "delitos de relación o por conexidad objetiva o medial" (Posada, 2017, p.102) con el manejo de datos que ponen en peligro la seguridad de la información, el patrimonio o la intimidad personal o familiar, entre otros.

Los delitos habilitados por la cibernética[1] son en esencia delitos tradicionales que pueden ampliarse en cuanto a su alcance o magnitud gracias al uso de computadoras, redes informáticas o cualquier otro tipo de TICs. Estos delitos son distintos de aquellos que solo dependen de la tecnología, y dos de los tipos más frecuentes son el fraude y la estafa informática. Sería el caso, por ejemplo, del delito de estafa (COIP, 2014, art.186) que se comete utilizando un correo electrónico para engañar a las víctimas y obtener un beneficio económico ilegal a través de la simulación de hechos falsos o deformación u ocultamiento de los hechos verdaderos. En este caso, se trata de un delito económico convencional, en donde la conducta de ingeniería social solo protege de manera marginal la seguridad de la información, los datos y los sistemas informáticos (FGE, 2021).

Además, en la era de la globalización informática, existen diversas amenazas para los usuarios del entorno digital a manos de delincuentes cibernéticos, que han llevado a la aparición de delitos ciber "(…) como el ciberterrorismo, ciberespionaje, ciberlavado o cyberlaundering, cibernacotráfico y la facilitación a la criminalidad organizada transnacional e internacional" (Posada, 2017, p. 47). No obstante, la existencia de disposiciones en el Código Orgánico Integral Penal que son válidas para conductas similares llevadas a cabo en terreno físico no implica que estas tampoco sean aplicables a acciones efectuadas mediante el uso de tecnologías de la información y comunicación (Muñoz, 2021).

Por el contrario, los delitos informáticos en sentido estricto o cibercrimen puro "son aquellos comportamientos ilícitos que se dirigen a la indebida creación, procesamiento, almacenamiento,

[1] La cibernética es el estudio de como los sistemas complejos afectan y luego se adaptan a su ambiente externo; en términos técnicos, se centra en funciones de control y comunicación: ambos fenómenos externos e internos del/al sistema. Esta capacidad es natural en los organismos vivos y se ha limitado en máquinas y organizaciones (Begoña, 2011).

adquisición, transmisión, divulgación, daño, falsificación, interceptación, manipulación previa o posterior, y ejecución automática de datos o sistemas informáticos sin el consentimiento o con abuso de este" (Posada, 2017, p. 104). Estos delitos afectan a nuevos intereses socialmente relevantes para los ciudadanos del ciberespacio, poniendo en peligro a bienes jurídicos como "confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde se almacenan o transfieren" (Acurio, 2003, p. 21). Es importante resaltar que "no se trata de delitos comunes sino de tipologías especiales realizadas a través de procedimientos informáticos, que gozan de cierta riqueza técnica, aunque no abandonan los tipos penales ordinarios como referentes dogmáticos y criminológicos" (Posada, 2017, p. 104).

En esta línea, estos delitos rompen los esquemas tradicionales, por lo que:

> "Con la expresión "delitos informáticos" suele aludirse a conductas que atentan de forma grave a determinados bienes del individuo –pero también de personas jurídicas–, que presentan una configuración específica y exclusiva de la actividad informática y telemática y han sido sometidos a una "tipología" "técnico-criminológica. […] pero lo que configura la originalidad del delito es precisamente la peculiaridad comisiva que ofrece el instrumento de ataque. En conclusión, la delincuencia informática o los delitos relacionados con ella indican un aspecto de la criminalidad caracterizado por una nueva dimensión que explica su especificidad; ambas notas las aportan los medios informáticos y telemáticos junto con sus funciones propias más importantes: el procesamiento y transmisión automatizados de datos y la confección y/o utilización de programas para tales. (Casabona citado por Posada, 2017, p. 105).

Es así como los delitos informáticos puros solo pueden ser perpetrados a través de la utilización de computadoras, redes informáticas o cualquier otra forma de tecnología de la información y comunicación. Estas acciones incluyen la propagación de virus o software malicioso, el hackeo y los ataques de denegación de servicios. Se distinguen por ser actividades ilícitas que están enfocadas principalmente en atacar computadoras o recursos de red, aunque pueden tener una variedad de efectos secundarios. Por ejemplo, los datos obtenidos a través del hackeo de una cuenta de correo electrónico pueden ser utilizados posteriormente para cometer fraudes informáticos.

En consecuencia, es importante tener en cuenta que la principal diferencia entre los delitos informáticos en sentido amplio y estricto radica en el papel que juegan las tecnologías de la información y los sistemas informáticos en el delito, el objetivo del ilícito y el modus operandi del cibercriminal. Cuando las TICs son el objetivo de la infracción, pueden verse afectadas negativamente la confidencialidad, integridad y disponibilidad de los sistemas y datos informáticos (UNODC, 2013), es decir que, el rol que cumplen los sistemas informáticos es esencial para la existencia de esta clase de delitos. Por otro lado, cuando las TICs son utilizadas como herramientas para el cometimiento de delitos tradicionales, tales como el fraude electrónico, la falsificación electrónica, la distribución de material de abuso sexual, se debe a la facilitación de las características propias del entorno digital.

Por lo tanto, es fundamental tener en cuenta los debates teóricos en el ámbito penal y la clasificación establecida por los convenios internacionales en materia de ciberdelincuencia, como el Convenio de Budapest sobre Ciberdelincuencia (2004). En el capítulo II, sección 1, este convenio clasifica los delitos informáticos en función de la conducta del ciberdelincuente y el objeto hacía donde se dirige la conducta ilícita: aquellos que atentan contra la confidencialidad, integridad y disponibilidad de los sistemas y datos informáticos, delitos informáticos, y aquellos relacionados con el contenido. Además, la Convención sobre Ciberdelincuencia incluye una definición para los delitos relacionadas con los derechos de autor y propiedad intelectual.

Esta clasificación no es completamente lógica, ya que no utiliza un solo criterio para separar las categorías. Tres de las categorías se refieren al objeto de la protección jurídica: “delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos”; “delitos relacionados con el contenido” y “delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines” (CSC, 2004). La categoría “delitos informáticos” no se refiere al objeto

de la protección jurídica sino al método. Esta falta de coherencia resulta en una cierta inconsistencia entre las categorías (UIT, 2009). Por lo que, varios términos que se emplean para describir actividades ilegales en línea, como el "ciberterrorismo" o la "pesca o phishing", se podrían incluir en varias categorías.

No obstante, las categorías establecidas en el Convenio sobre la Ciberdelincuencia son extremadamente importantes para discutir sobre el fenómeno de la ciberdelincuencia. Aunque el Ecuador aún no forma parte de esta Convención, ha sido una fuente fundamental para la armonización y tipificación de estos delitos en el Código Orgánico Integral Penal. A diferencia de otras legislaciones, el ordenamiento jurídico penal en Ecuador ha sufrido un retraso en los últimos tiempos en materia de delitos informáticos. De hecho, el anterior Código Penal data de 1938, lo que representa una brecha de 70 años hasta la reciente promulgación del Código Orgánico Integral Penal. Con la entrada en vigor de este último código, los operadores de justicia han podido enfrentar la creciente criminalidad informática, que se aprovecha cada vez más del uso de la informática en casi todas las áreas de la vida social. Anteriormente, muchas de estas conductas delictivas quedaban impunes, ya que no estaban reguladas en el Código Penal anterior, como el caso de la pornografía infantil (FGE, 2021).

a) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Esta clasificación se compone de los delitos informáticos en sentido estricto, es decir, aquellos ataques dirigidos a los sistemas informáticos, redes y datos con el objetivo de lesionar o poner en peligro a la confidencialidad, integridad y disponibilidad de los datos o sistemas informáticos. Esto incluye conductas donde un tercero accede a datos o información que se encuentra protegida y solo puede ser accedida legítimamente por el usuario o propietario de la información. La integridad

de la información se refiere a la confiabilidad y precisión de los datos, lo que significa que los datos o información no han sido modificados o dañados por terceros no autorizados. La disponibilidad de la información se centra en la accesibilidad del usuario a los datos, servicios o sistemas informáticos.

A pesar de que en la legislación penal ecuatoriana se ha contemplado delitos como el robo o el homicidio durante siglos, la inclusión de los delitos informáticos en la misma es reciente, dado que los sistemas y datos informáticos sólo surgieron hace unas pocas décadas (UIT, 2009). La digitalización de los datos ha aumentado la importancia de estos, lo que ha llevado a un aumento en los ataques informáticos. Estos ataques incluyen desde el acceso ilegal a sistemas informáticos hasta el espionaje de datos a través de softwares maliciosos. La venta ilegal de la información personal y financiera es altamente cotizada en los mercados negros en línea, que pueden ser utilizados para obtener acceso no autorizado a cuentas bancarias y tarjetas de crédito.

Por lo tanto, se han tipificado y sancionado diversas conductas en el Código Orgánico Integral Penal relacionadas con los delitos informáticos en sentido estricto con el objetivo de proteger a este nuevo bien jurídico la "seguridad de los datos, la información y las funciones de los sistemas informáticos" (Posada, 2017, p. 34). Con la incorporación del Código Orgánico Integral Penal en el 2014, se agrega una nueva categoría delitos: "delitos contra la seguridad de los activos de los sistemas de información y comunicación".

Dentro de esta categoría, se incluyen actividades ilícitas como el hacking, la creación, desarrollo, programación, adquisición o envió de software malicioso" (COIP, 2014, art. 232), ataques de denegación de servicios (DoS), ataques de denegación de distribución de servicios (DDoS), entre otros delitos.

La doctrina especializada en el tema ha acuñado el término "hacking" o "piratería informática" para referirse al acceso ilícito a un sistema informático, siendo considerado uno de los delitos más antiguos en este ámbito (UIT, 2009). En la legislación penal ecuatoriana, este delito se encuentra tipificado como "acceso no consentido a un sistema informático, telemático o de telecomunicaciones" en el artículo 234 del Código Integral Penal, mismo que señala que:

> 1. La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho sobre dicho sistema, será sancionada con la pena privativa de la libertad de tres a cinco años (COIP,2014).

Los primeros hackers amaban la tecnología y buscaban expandir los límites de los programas. La palabra hacker no tenía connotación negativa en ese entonces (Jahankhani, Al-Nemrat, Hosseinian-Far, 2017). Hoy en día, el cibercrimen ha evolucionado a un modelo de servicio corporativo, en el cual los delincuentes ofrecen sus habilidades y esperan ser contratados a cambio de un pago. Los motivos de los ciberdelincuentes varían dependiendo del objetivo, estos pueden ser económicos, políticos o sociales. “Algunos se limitan a burlar las medidas de seguridad para probar sus capacidades” (UIT, 2009, p.22). Otros individuos realizan actividades de hacking por motivos relacionados con la política o la sociedad, como es el caso del grupo de hacking Anonymous, que opera sin una autoridad centralizada.

Adicionalmente, el legislador no menciona la autorización o voluntad por casualidad, ya que, como señala Lusthaus (2018), "no todo ciberdelincuente es hacker, y viceversa" (p. 11). Los primeros hackers fueron científicos informáticos e intelectuales curiosos que experimentaban con prototipos de computadoras en universidades (Lusthaus, 2018). Según Acurio (2002), "la misión de un hacker nunca es destruir, causar daño o beneficiarse económicamente de la información a la que acceden de manera no autorizada" (p. 67), ya que estas acciones son características de los llamados crackers o piratas informáticos.

En todo caso, el acceso ilícito a un sistema informático a menudo es solo un medio, aunque relevante, para realizar otras actividades ilícitos, como fraudes y falsificaciones informáticas. En este sentido se establece en el artículo 234 numeral 2 del Código Orgánico Integral Penal una conducta adicional: "explotar ilegítimamente el acceso logrado" (COIP,2014) para modificar un portal web, desviar o redireccionar el tráfico de datos o voz.

De igual manera, el informe explicativo de la Convención de Budapest del 2001 contra el cibercrimen establece la definición de acceso ilícito:

> […] el delito básico que constituyen las amenazas peligrosas y los ataques a la seguridad (es decir, contra la confidencialidad, la integridad y la disponibilidad) de los sistemas y datos informáticos. La necesidad de protección refleja los intereses de las organizaciones y las personas para manejar, operar y controlar sus sistemas sin interrupciones ni restricciones. La mera intromisión no autorizada, es decir, la "piratería" (hacking), el "sabotaje" (cracking) o "la intrusión en el ordenador" (computer trespass) debería en principio ser ilícita en sí misma. (p.13)

En visto de ello, se debe tener en cuenta que el acceso no consentido a sistemas informáticos, telemáticos o de telecomunicaciones suele ser utilizado como un delito medio para cometer otros cibercrímenes. En el ámbito jurídico, se exige que se violen las medidas de seguridad con intención deshonesta para modificar, desviar o redirigir datos informáticos de los sistemas o cualquier otra tecnología de la información y comunicación. Actualmente, los grupos de ciberdelincuencia organizada tienen los recursos para contratar a las personas necesarias, lo que hace que la amenaza del crimen organizado y terrorismo sea cada vez más sofisticada al aumentar la capacidad de infiltrar, controlar y desestabilizar los sistemas informáticos y de seguridad.

Por otro lado, la interceptación ilícita representa una transgresión a la privacidad equiparable a la grabación de conversaciones telefónicas entre remitente y destinatario. Los cibercriminales pueden intervenir mensajes de correo electrónico o redes sociales, o interceptar datos informáticos

para registrar el cambio de información. La tipificación de este delito busca proteger la privacidad de la comunicación, los datos o la información.

Hoy en día, la transmisión de datos hacía, desde o dentro de un sistema informático es un componente crucial de la vida moderna en línea. Desafortunadamente, los ciberdelincuentes están siempre buscando formas de explotar los puntos débiles del sistema. En algunas circunstancias, puede ser relativamente sencillo para ellos interceptar las comunicaciones si la red o la comunicación no están adecuadamente protegidas. Cuando se interceptan estas comunicaciones, puede hacer pública información personal sensible, como contraseñas de cuentas bancarias, tráfico de red, chats privados y sitios web visitados recientemente.

Esta actividad ilícita radica en el:

> […] hecho de interceptar datos informáticos personales (datos sensibles, privados o semiprivados de naturaleza económica) o impersonales (aquellos no referidos a personas pero que no resultan anónimos, etcétera), bien en el sistema informático de donde provienen (origen) durante su transmisión no pública por canales físicos o inalámbricos Wi-Fi, o en el sistema informático a donde son enviados (destino). (Posada, 2017, p. 273)

En la legislación penal ecuatoriana, este delito se encuentra tipificado como "interceptación ilegal de datos" en el artículo 230 del Código Orgánico Integral Penal, mismo que señala que:

> Será sancionada con pena privativa de libertad de tres a cinco años:
>
> 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma, contenido digital en su origen, destino o en el interior de un sistema informático o dispositivo electrónico, una señal o una transmisión de datos o señales.
>
> 2. La persona que ilegítimamente diseñe, desarrolle, ejecute, produzca, programe o envíe contenido digital, códigos de accesos o contraseñas, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente al que quiere acceder.
>
> 3. La persona que posea, venda, distribuya o, de cualquier otra forma, disemine o introduzca en uno o más sistemas informáticos, dispositivos electrónicos, programas u otros contenidos digitales destinados a causar lo descrito en el número anterior.

> 4. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
>
> 5. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos, o programas o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior. (COIP, 2014)

El delito de interceptación ilegal de datos consiste en la interceptación dolosa de datos o comunicaciones informáticas sin la debida autorización judicial. Este tipo de delito se caracteriza por tener un "sujeto activo monosubjetivo y común" (Posada, 2017, p. 275), lo que significa que cualquier individuo puede ser considerado autor del delito. Su finalidad radica en proteger la confidencialidad, integridad y disponibilidad de la información, datos, señales y sistemas informáticos.

De acuerdo con Posada (2017), la interceptación ilegal de datos es considerado como un "delito pluriofensivo" (p. 277), ya que el tipo penal involucra la violación no consensuada de la seguridad de la información y las funciones informáticas. Específicamente, el delito se refiere a la interceptación no autorizada de transmisiones de datos no públicos (tanto emisiones como recepciones) a través de sistemas informáticos y redes de comunicación, y exige el tratamiento confidencial, seguro, confiable e integro de dicha información. Además, la interceptación ilegal de datos tiende a afectar de manera negativa al derecho fundamental a la intimidad personal y familiar de aquellos que son titulares de los datos informáticos.

En este sentido, la resolución A/c.3/68/L.45/REV.1 de la Asamblea de las Naciones Unidas (2013) ha señalado que:

> La vigilancia y la interceptación ilícita o arbitraria de las comunicaciones, así como la recopilación ilícita o arbitraria de datos personales, al constituir actos de intrusión grave, violan los derechos a la privacidad y a la libertad de expresión y pueden ser contrarios a los preceptos de una sociedad democrática. Y, afirma que los derechos de las personas también deben estar protegidos en Internet, incluido el derecho a la privacidad. (p. 11)

Precisamente, esta conducta ilícita vulnera de manera abusiva o violenta, no solo el bien jurídico de la seguridad de las funciones informáticas como la "confiabilidad, confidencialidad, integridad, disponibilidad, el no repudio y la recuperación de los sistemas informáticos, los datos allí registrados, sino también el habeas data, esto es, el derecho a la libre disposición, inviolabilidad, almacenamiento y transmisión de datos e información digital" (Posada, 2017, p. 278). En el caso del Ecuador, el habeas data se refiere a una garantía jurisdiccional la cual se encuentra reconocida en el artículo 92 de la Constitución del Ecuador, que tiene como finalidad "conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma" (CRE, 2008).

Imagen 1
Man in the Middle (MITM) Attack: Learn About Man-in-the-Middle Attacks, Vulnerabilities, and How to Prevent MITM Attacks

Veracode, 2016

A manera de ejemplificación, los ataques de intermediario (también conocidos como "Man- in-the-Middle" o "MITM") se adecuan a lo establecido en el artículo 230 del Código Orgánico Integral Penal. Esta clase de ciberataques consisten en que el ciberdelincuente aparenta ser un intermediario legítimo, que se sitúa entre la comunicación de dos partes con la finalidad de interceptar, manipular o robar información, por lo tanto, las víctimas no son conscientes de lo que ha ocurrido hasta que se percatan de que su comunicación se ha visto comprometida.

El ataque de intermediario puede adoptar diversas formas, por ejemplo, cuando se realiza la creación de puntos de acceso WI-FI falsos, la instalación de software malicioso en los dispositivos

electrónicos o la explotación de vulnerabilidades en los sistemas de red para interceptar las comunicaciones. Una vez que el ciberdelincuente ha interceptado la comunicación podrá espiar, robar o manipular los datos informáticos, con la finalidad de obtener contraseñas, información financiera o datos personales.

Igualmente, en la normativa penal ecuatoriana se contemplan aquellas conductas que atentan contra la integridad de los sistemas informáticos. Esto se debe a que cada vez más empresas incorporan sus bienes y servicios en la red, lo que les permite tener una disponibilidad global. Al impedir el correcto funcionamiento de los sistemas informáticos, los ciberdelincuentes pueden causar pérdidas económicas a las empresas. La importancia de esta disposición es "proporcionar a los datos informáticos y a los programas informáticos una protección similar a la que gozan los objetos corpóreos contra la imposición de un daño deliberado" (CSC, 2004, p.17).

En la legislación penal ecuatoriana, este delito se encuentra tipificado como "ataque a la integridad de sistemas informáticos" en el artículo 232 del Código Orgánico Integral Penal, mismo que señala que:

> La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento o comportamiento no deseado, o suprima total o parcialmente contenido digital, sistemas informáticos, sistemas de tecnologías de la información y comunicación, dispositivos electrónicos o infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general, con el propósito de obstaculizar de forma grave, deliberada e ilegítima el funcionamiento de un sistema informático, será sancionada con pena privativa de libertad de tres a cinco años.
>
> Con igual pena será sancionada la persona que diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos, programas o sistemas informáticos maliciosos o destinados a causar los efectos señalados en el primer inciso de este artículo.
>
> Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad. (COIP,2014)

"El interés legal protegido en este caso es la integridad y correcto funcionamiento de los datos y programas informáticos" (CSC, 2004, p. 17). Es importante considerar que, si alguien con intenciones maliciosas tiene la posibilidad de acceder físicamente a un sistema informático, podría provocar su destrucción, aunque este tipo de daño físico no representa un problema mayor ya que es similar a los casos de daño a bien ajeno. Sin embargo, en el contexto de las empresas que brindan servicios de e-commerce, las consecuencia financieras derivadas de los ataques informáticos a sus sistemas suelen ser más significativas que el valor de los equipos informáticos afectados.

A manera de ejemplificación, los ataques DDoS interfieren con el "sistema al sobrecargar el servidor o intermediario (p.ej., los enrutadores) con solicitudes para impedir que el tráfico legítimo acceda a un sitio web o use un sistema" (Maras, 2016, p. 270), afectando de esa manera a la integridad y el correcto funcionamiento de los sistemas informáticos. Esta conducta se adecua a lo dispuesto en el artículo 232 del Código Orgánico Integral Penal.

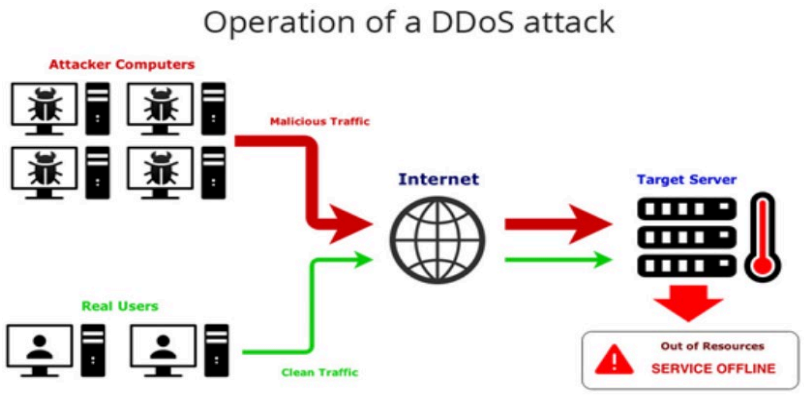

Imagen 2
Operaciones de ataques DDoS
Nextvision, 2018

De ahí que, un ataque de denegación de distribución de servicios se refiera al "uso de múltiples computadoras y otras tecnologías digitales que permiten la coordinación de ataques con el fin de sobrecargar los servidores o intermediarios para impedir el acceso de los usuarios legítimos"

(Maras, 2016, p. 270). Los ciberdelincuentes utilizan una red de sistemas informáticos infectados (botnets) para conectarse a un solo servidor y enviar solicitudes falsas para colapsarlo, como se muestra en la imagen número 2.

Los cibercriminales que se dedican a realizar "DDoS extorsión" operan de esta manera: primero infectan varios dispositivos con software malicioso para tomar el control sin el consentimiento del usuario. Luego, utilizan estos dispositivos infectados para llevar a cabo ataques de denegación de distribución de servicios de manera remota y controlada. Esto se logra mediante el uso de redes zombi o botnets que envían solicitudes maliciosas con el objetivo de colapsar el funcionamiento de los servidores.

Es así como los ciberataques realizados a la integridad de los sistemas informáticos pueden ser llevados a cabo por diversos actores, como individuos con aspiraciones personales, hackers, piratas informáticos, grupo de ciberdelincuencia organizada o incluso Estados nación. Cada actor tiene su propia variabilidad, lo que puede tener un impacto significativo en la afectación de los sistemas informáticos. Por ejemplo, un Estado puede llevar a cabo un ataque a las infraestructuras esenciales de otro Estado, como el sector energético, financiero, sanitario u otros servicios, incidiendo de esta manera en forma negativa a la calidad de vida de los ciudadanos del país afectado y poniendo de esta manera en peligro a la seguridad nacional de un Estado.

Además, de los delitos mencionados, el Código Orgánico Integral Penal reconoce como delitos informáticos en sentido estricto la revelación ilegal de base de datos y los delitos contra la información pública reservada legalmente. En la actualidad, los sistemas informáticos contienen información reservada y los ciberdelincuentes tratan de obtenerla por Internet desde cualquier lugar del mundo. “El valor de la información confidencial y la capacidad de acceder a la misma a distancia hacen que el espionaje de datos resulte muy interesante” (UIT, 2004, p. 24).

Imagen 3
Valor de los datos en la darknet
Kaspersky, 2021

Actualmente, los ciberdelincuentes tienen como objetivo principal obtener secretos comerciales, pero también están dirigiendo sus ataques cada vez más hacia los sistemas informáticos privados. Los usuarios privados almacenan en sus computadoras información confidencial, como datos financieros, lo que puede ser utilizado por los cibercriminales para beneficio propio o vendido a terceros. Se han creado mercados negros en línea donde se venden datos de tarjetas de crédito como ejemplo de esta práctica.

b) Delitos informáticos

La doctrina especializada en el tema define a los delitos informáticos como infracciones comunes que se llevan a cabo a través de la utilización de dispositivos electrónicos, sistemas informáticos o telemáticos. De la misma manera, esta categoría se encuentra íntimamente ligada con los delitos informáticos en sentido amplio, es decir, “aquellas conductas punibles que pueden ser realizadas mediante el empleo de medios informáticos, electrónicos o telemáticos.” (FGE, 2021, p. 23).

Por lo que, debido a las características propias de los sistemas informáticos permiten al ciberdelincuente lograr un mayor impacto en el Internet generando daños personales y económicos a los usuarios digitales. Estos delitos son frecuentes y los sistemas informáticos y las tecnologías de la información y comunicación son herramientas esenciales para los ciberdelincuentes. A diferencia de la categoría anterior, estos delitos tienden a ser más flexibles en la protección de principios jurídicos (CSC, 2004).

De acuerdo con la clasificación presentada en el estudio exhaustivo sobre el delito cibernético de la UNODC (2013) se identifican las siguientes conductas dentro de esta categoría:

- Fraude y falsificación informática
- Delitos informáticos relacionados con la identidad
- Envío y control del envío de correo basura
- Delitos informáticos de derechos de autor y marcas comerciales
- Actos relacionados con la informática que causen daño personal
- Instigación o «captación de niños con fines sexuales» por medios informáticos. (p. 16)

En el caso de los fraudes informáticos estos son "de los delitos más populares cometidos por Internet" (UIT, 2004, p. 49). El anonimato que proporciona el Internet es relevante a la hora de cometer esta clase de ilícitos, debido a que el ciberdelincuente puede encubrir su identidad de manera sencilla con la automatización y desarrollo de herramientas informáticas. "Estos delitos consisten principalmente en manipulaciones respecto de la introducción de datos, cuando se introducen datos incorrectos en un ordenador, o en manipulaciones respecto de los programas y otras interferencias al procesamiento de los datos" (CSC, 2008, p. 23).

En relación con esto, la dogmática penal está debatiendo si la transferencia electrónica de activos patrimoniales debe ser considerada como una forma de delito distinta a la estafa convencional, siendo este el punto de partida para su análisis. La respuesta es negativa y depende de dos factores.

> Primero, porque se trata de un verdadero cibercrimen que, a diferencia del delito de hurto por medios informáticos, no remite su supuesto de hecho y la pena a otros delitos patrimoniales, naturalmente, sin perjuicio de compartir algunos elementos o características con ellos. Por el contrario, otros autores consideran que la transferencia de activos en realidad es una modalidad especial del delito de estafa, y así lo afirman siendo coherentes con ordenamientos que consagran los delitos informáticos defraudatorios como modalidades de estafa.
>
> Y, segundo, porque se advierten claras diferencias dogmáticas (objetivas y subjetivas) entre la estafa común y la transferencia no consentida de activos que, precisamente, se caracteriza por castigar las defraudaciones (no constitutivas de apoderamientos de cosas muebles) realizadas por medio de la manipulación de sistemas informáticos. (Posada, 2017, p. 397)

En el capítulo previo se indicó que una de las dificultades asociadas con la clasificación de los delitos informáticos en el Convenio de Budapest se debe a que acciones como el ciberterrorismo o el fraude informático pueden entrar dentro de diferentes categorías. Es el caso, del fraude informático o transferencia electrónica de activo patrimonial que está tipificado en la sección tercera, delitos contra la seguridad de los activos informáticos y de la comunicación, artículo 231 del Código Orgánico Integral Penal:

> **Transferencia electrónica de activo patrimonial. -** La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.
>
> Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona. (COIP, 2014)

De igual manera, esta clase de defraudaciones se encuentran tipificadas de la siguiente manera en el artículo 8 del Convenio de Budapest:

> **Fraude informático. -** Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de:
>
> a. la introducción, alteración, borrado o supresión de datos informáticos
>
> b. cualquier forma de atentado al funcionamiento de un sistema informático,

> con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero. (CSC, 2004)

La principal diferencia entre el fraude informático y el fraude tradicional es la finalidad que acecha el ciberdelincuente. Cuando un estafador intenta manipular o engañar a un humano, es considerado un fraude tradicional. Por otro lado, si el objetivo es el sistema informático o de procesamiento de datos, se trata de un fraude informático.

De la misma manera, en esta categoría de delitos se encuentra la "falsificación informática" o "falsedad informática" que implica la manipulación de documentos digitales (UIT,2009), es considerado como un acto preparatorio para realizar otros ciberdelitos, pues tiene como verbos rectores "introducir, modificar, eliminar o suprimir contenido digital" (COIP, 2014, art. 234.1); y, "en la manipulación o el uso malicioso de los resultados pertinentes de un proceso de elaboración de datos almacenados, mediante la configuración de los programas de software" (Posada, 2017, p. 177). De acuerdo con la doctrina especializada, también se incluirán las modificaciones, eliminación y cambios realizados posteriormente en datos o documentos informáticos genuinos y relevantes, ya sean públicos o privados y que se encuentren registrados en sistemas informáticos.

Desde el punto de vista técnico e informático, la falsedad informática es una conducta que afecta "la integridad, veracidad y confiabilidad del contenido de los datos informáticos y de las funciones informáticas, en especial las del sistema infectado, y buscan que la información falsa generada tenga legitimidad en el tráfico documental digital" (Posada, 2017, p. 178). Este ilícito se encuentra tipificado en la Convención de Budapest, capitulo II, sección 1, art. 7:

> Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos, con independencia de que sean directamente legibles e inteligibles. Los Estados podrán reservarse el derecho a exigir la concurrencia

> de un ánimo fraudulento o de cualquier otro ánimo similar para que nazca responsabilidad penal. (CSC, 2004)

De acuerdo a lo señalado en el reporte explicativo de la Convención del Cibercrimen del Consejo de Europa, la finalidad de tipificar y sancionar en el derecho interno el delito de falsificación informática es:

> […] establecer un delito paralelo al de falsificación de documentos tangibles. Su objetivo es colmar algunas lagunas en el derecho penal en relación con el delito de falsificación tradicional, que requiere la legibilidad visual de las afirmaciones o declaraciones contenidas en un documento y que no se aplica a los datos almacenados electrónicamente. Las manipulaciones de dichos datos con valor probatorio pueden tener las mismas consecuencias graves que los actos de falsificación tradicionales si un tercero se ve así engañado. (CSC, 2008, p. 22)

Al igual que los fraudes informáticos, el delito de falsificación informática puede ser concebida desde dos categorías: delitos informáticos o delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. En el caso del derecho interno, este ilícito se encuentra tipificado en la sección III, delitos contra la seguridad de los activos de la información y comunicación, artículo 234. 1:

> 1. La persona que, con intención de provocar un engaño en las relaciones jurídicas, introducir, modificar, eliminar o suprimir contenido digital, o interferir de cualquier otra forma en el tratamiento informático de datos, produzca datos o documentos no genuinos, será sancionada con pena privativa de libertad de tres a cinco años.
>
> 2. Quien, actuando con intención de causar un perjuicio a otro o de obtener un beneficio ilegitimo para sí o para un tercero, use un documento producido a partir de contenido digital que sea objeto de los actos referidos en el número 1, será sancionado con la misma pena. (COIP, 2014)

La falsificación informática puede tomar diferentes formas, una de ellas es la usurpación de dominios web, lo que implica crear páginas web similares a las originales para que los usuarios ingresen sus contraseñas o credenciales en el dominio falso. Para lograr esto, los ciberdelincuentes utilizan técnicas de ingeniería social para conocer a su víctima. La ingeniería social se refiere a la manipulación, engaño, influencia o estafa de los individuos con la finalidad de que revelen información privada que resulten en un beneficio para el ciberdelincuente (Maras, 2016).

Tradicionalmente, esta clase de conductas ilícitas las realizan los ciberdelincuentes como acto preparatorio para obtener información confidencial del usuario, como contraseñas, nombres e información bancaria, suplantando la identidad o haciéndose pasar por un medio confiable y seguro. Estos actos implican el uso de botnets para enviar de manera masiva correos fraudulentos que parecen ser mensajes auténticos de organizaciones públicas o privadas, agencias financieras o personas confiables, con el objetivo de ganar la confianza del usuario. Estos correos electrónicos suelen ser identificables debido a la poca variación en los dominios o direcciones originales.

Además de los mencionados, el estudio exhaustivo sobre el delito cibernético de la UNODC (2013) también hace referencia a los actos relacionados con la informática que causan daño personal, considerando como actos ilícitos aquellos que mediante "el uso de un sistema informático hostigan, abusan, amenazan, acosan o causan miedo o intimidación a una persona" (p. 17). Algunos ejemplos de estos tipos de delitos informáticos que casan daño a un persona a través de sistemas informáticos son el "acecho cibernético, el hostigamiento cibernético y el ciberacoso" (UNODC, 2013, p. 18).

De acuerdo con Maras (2016) se incluye las siguientes definiciones en la que se menciona elementos particulares de cada delito:

1. **Acecho cibernético:** El uso de las tecnologías de la información y comunicación (TIC) para cometer una serie de actos de manera reiterada con el fin de hostigar, atacar, amenazar, asustar, o abusar de forma verbal a un individuo (o individuos).
2. **Hostigamiento cibernético:** El uso de las tecnologías de la información y comunicación (TIC) para humillar, acosar, atacar, amenazar, asustar, ofender o abusar de forma verbal de un individuo (o individuos) intencionalmente.
3. **Ciberacoso:** El uso de las tecnologías de la información y comunicación (TIC) por niños para humillar, acosar, insultar, hostigar, asustar, ofender, acosar, abusar o de cualquier forma atacar a otro niño o niños (p. 33).

En la legislación penal ecuatoriana, el ciberacoso sexual es considerada como una forma de comisión circunstancial que no forma parte de la definición del tipo penal fundamental, siendo el caso del delito de acoso tipificado y sancionado en el artículo 166 del Código Orgánico Integral:

> […] Se considerará ciberacoso sexual cuando la conducta descrita en el inciso anterior se realice utilizando cualquiera de las tecnologías de la información y comunicación, medios tecnológicos, electrónicos o digitales, y será sancionado con una pena privativa de libertad de uno a cinco años. (COIP, 2014)

La particularidad de los delitos informáticos que causan daños personales es la edad de los perpetradores, la intensidad y prevalencia del delito (UNODC, 2018). Varios cibercriminales dedicados a la captación de menores con fines sexuales se aprovechan del anonimato que la red provee para promover la confianza de sus potenciales víctimas, en estos casos y de manera grave, dirigidos hacia de niños, niñas o adolescentes. Mediante la manipulación del menor o adolescente el ciberdelincuente promueve un modelo de confianza con fines sexuales, por lo general, se lo realiza en plataformas como las redes sociales, correos electrónicos, salas de chat online, entre otras (Muñoz, 2021, p. 38). A esta conducta la doctrina especializada en el tema la ha denominado como *child grooming* o de manera específica "contacto con finalidad sexual con menores de dieciocho años por medios electrónicos", misma que tiene como finalidad lograr "un proceso en el cual se configuran una serie de tácticas que buscan conseguir un acercamiento con el menor, ganar su confianza y lograr un encuentro físico para perpetrar conductas lesivas de índole sexual" (O'Connell, 2003, p. 72).

El delito de contacto con finalidad sexual con menores de dieciocho años por medios electrónicos o grooming no es ajeno a la problemática de la sociedad ecuatoriana, pues, de acuerdo con el Sistema Integrado de Actuaciones Fiscales (SIAF) de la Fiscalía General del Estado, este delito cibernético ha sido denunciado en reiteradas ocasiones.

Art. COIP.	Tipo Penal	2017	2018	2019	2020	2021	TOTAL
174 inc. 2	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	12	14	16	7	7	**56**

Imagen 4
DATOS SIAF
FGE, 2021

En cuanto al bien jurídico protegido en el delito de contacto con finalidad sexual con menores de dieciocho años por medios electrónicos, la doctrina especializada señala que esta busca "protección de la indemnidad sexual, entendida como el normal desarrollo y formación de la vida sexual de aquellas personas que, de acuerdo a la legislación, no poseen aún edad para determinar válidamente su comportamiento en el ámbito sexual" (FGE, 2021, p.12).

c) Delitos relacionados con el contenido

Los delitos informáticos relacionados con el contenido son conductas ilícitas que se cometen a través de medios informáticos y se encuentran relacionados con el contenido ilegal, como la difusión de material de abuso sexual infantil, el discurso de odio, la incitación a la violencia, la discriminación racial o religiosa, la difamación y la calumnia. En todos estos casos, el uso de la tecnología y de los medios digitales se convierte en una herramienta para llevar a cabo estos delitos de manera más eficiente y a menudo de manera anónima. El objeto material del delito "suele ser una persona, un grupo identificable de personas, o un valor o creencia bastante difundido" (UNODC, 2014, p. 99). Además, los actores de estos delitos pueden ser realizados de forma individual o grupal generando graves consecuencias para las víctimas y la sociedad en general.

Es así como la incorporación de estos delitos en la legislación penal interna puede verse influenciado principalmente por perspectivas nacionales, las cuales tienen en cuenta factores

políticos o culturales, ya que, en cuanto al contenido ilícito, los valores y sistemas jurídicos pueden diferir entre cada sociedad. Por ejemplo, "la utilización de comentarios despectivos al referirse al Sagrado Profeta se considera un acto criminal en muchos países islámicos, pero no en algunos países" (UIT, 2009, p. 32).

Uno de los delitos más graves relacionados con el contenido es la producción y distribución de material de abuso sexual infantil. Este delito no solo implica la explotación sexual de niños, niñas o adolescentes, sino que también puede ser utilizado para el chantaje y la extorsión de las víctimas. Además, la distribución de este tipo de contenido puede tener consecuencias graves en la salud mental y emocional de los menores de edad involucrados. Para *International Centre for Missing & Exploited Children (ICMEC)* (2018) se debería emplear el término de "material de abuso sexual infantil", en vez de pornografía infantil, debido a que dicho término minimiza la gravedad estos delitos.

En este sentido, el reporte explicativo de la Convención de Cibercrimen del Consejo de Europa ha señalado que la finalidad de tipificar y sancionar en el derecho interno los delitos relacionados con material de abuso sexual infantil es:

> […] reforzar las medidas de protección de los menores, incluida su protección contra la explotación sexual, mediante la modernización de las disposiciones del derecho penal con el fin de circunscribir de manera más eficaz la utilización de los sistemas informáticos en relación con la comisión de delitos de índole sexual contra menores. (CSC, 2008, p. 24)

En la legislación penal ecuatoriana, los delitos relacionados con la pornografía infantil se encuentran tipificados y sancionados en los artículos 103 y 104 del Código Orgánico Integral Penal. Se sanciona aquellas personas que "fotografíen, filmen, graben, produzcan, transmitan o editen material que contenga la representación visual de niños, niñas o adolescentes desnudos o semidesnudos". (COIP, 2014, art. 103) La comercialización de material de abuso sexual infantil

abarca aquellas conductas que estén relacionadas con la publicidad, compra, posesión, porte, transmisión, descarga, almacenamiento, importe, exporte o venta, por cualquier medio, para uso personal o intercambio.

La tipificación de estos delitos tiene como objetivo proteger la indemnidad, seguridad, derecho a la propia imagen, la intimidad y a la dignidad de la infancia en abstracto. Además, con esto, se pretende adelantar "las barreras de protección y atacar el peligro inherente a conductas que pueden fomentar prácticas pedofílicas sobre niños, niñas o adolescentes concretos" (Corte Nacional de Justicia, Segunda Sala de Casación Penal, 2014, fj.10).

Lamentablemente, de acuerdo con las estadísticas del Sistema Integrado de Actuaciones Fiscales (SIAF) de la Fiscalía General del Estado los delitos relacionados con material de abuso sexual infantil han sido denunciados en reiteradas ocasiones, por lo que esta clase de delitos no son ajenos a la sociedad ecuatoriana.

Art. COIP.	Tipo Penal	2017	2018	2019	2020	2021	TOTAL
103	Pornografía con utilización de niñas, niños o adolescentes	103	104	81	113	95	**496**
104	Comercialización de pornografía con utilización de niñas, niños o adolescentes	26	9	17	18	15	**85**

Imagen 5
DATOS SIAF
FGE, 2021

Otro delito informático relacionado con el contenido es el "ciberterrorismo", pues todo cambio a partir de la tragedia de los atentados al World Trade Center. Desde entonces, "se entabló un

intenso debate sobre la utilización de las TIC por lo terroristas, propiciado por informes que revelaban el uso de Internet en la preparación del ataque" (UIT, 2009, p.57). A pesar de que no se trataron de ciberataques, ya que el grupo responsable de los ataques no los llevó a cabo a través de Internet, sino que utilizó en la planificación de estos. En la actualidad se conoce que los grupos terroristas acuden a las TIC y a Internet para los siguientes fines:

- Propaganda (incluidos el reclutamiento, radicalización y la instigación al terrorismo);
- Financiación de actividades terroristas
- Adiestramiento
- Planificación de ataques en el mundo real (tanto por medio de comunicaciones secretas, como mediante información de dominio público)
- Ejecución y coordinación de los ataques
- Ataques contra infraestructuras esenciales (abarcan los ataques cibernéticos). (UNODC, 2014, p.104)

Como tal esta categoría de delitos, se enfoca únicamente en el contenido informático relacionado con el terrorismo y no incluye las amenazas de ciberataques por parte de grupos terroristas.

Por lo tanto, para prevenir y combatir los delitos informáticos relacionados con el contenido, es relevante que existan leyes y regulaciones claras que establezcan qué es ilegal y qué no lo es en el ámbito digital. También es importante educar a las personas sobre el uso ético de la tecnología, así como fomentar la denuncia de este tipo de delitos para que puedan ser investigados y sancionados adecuadamente por las autoridades competentes.

En conclusión, los delitos informáticos relacionados con el contenido son una amenaza grave en el ámbito informático, y es necesario que existan medidas efectivas para prevenir y combatir este tipo de delitos. La educación, la regulación y la denuncia son fundamentales para proteger a la sociedad de los efectos perjudiciales de estos delitos.

1.2. Ciberdelincuencia organizada y el fenómeno de la corporativización del cibercrimen.

En la actualidad, el concepto de delincuencia organizada ha sido alterado por el impacto de las tecnologías de la información y comunicación. En particular, las TIC han tenido una influencia en la naturaleza de las actividades llevadas a cabo por grupos criminales organizados y en la variedad de individuos que pueden formar parte de ellos. Esta transformación no solamente se refiere a los cambios en los tipos de delitos cometidos y en los métodos empleados por estos grupos, sino también a la diversidad de personas que pueden verse involucrados (UNODC, 2022). Es así como en las últimas décadas, el cibercrimen ha evolucionado de ser una actividad realizada por individuos aislados a una forma organizada de delincuencia corporativa.

Con la corporatización de los delitos informáticos, estos se realizan de forma organizada y profesional, sin motivaciones personales más allá de obtener ganancias económicas. La víctima del delito se considera como un elemento fungible y sin interés para el ciberdelincuente. La búsqueda de beneficios a través del abuso de las herramientas tecnológicas ha hecho que el cibercrimen sea un negocio rentable (Muñoz, 2021, p. 42). Según el subdirector asistente de la división cibernética del FBI, Steven R. Chabinsky (2011), esto se ha vuelto cada vez más evidente, pues:

> […] al igual que con otras actividades ilícitas que se han vuelto más organizadas y profesionales, como el tráfico de personas y el tráfico de armas, los ciberdelitos graves están siendo dominados por delincuentes que se ven a sí mismos como hombres de negocios... y el cibercrimen es su negocio […]. (p.1)

Según Jonathan Lusthaus en su obra "The corporatisation of cybercrime", hay tres factores clave para explicar este fenómeno. El primero se debe a la arquitectura de Internet y su evolución, que ha permitido una mayor congregación y colaboración en línea. La corporatización del cibercrimen dependió, al menos en parte, del desarrollo de recursos de comunicación, ya que, de lo contrario, la colaboración y organización en línea habrían sido difíciles (Lusthaus, 2012).

En segundo lugar, el aumento de la seguridad informática en los últimos años que paradójicamente ha dificultado el hacking por hobby y ha llevado al cibercrimen hacia la profesionalización impulsada por los réditos económicos. Actualmente la situación de la seguridad informática se ha endurecido considerablemente, ha habido una gran disminución en el número de hackers por hobby (Lusthaus, 2012).

En tercer lugar, y quizá la más importante, el traslado de operaciones comerciales y datos financieros y personales al ciberespacio ha creado un enorme potencial de ganancias para los cibercriminales. Los datos informáticos son un objetivo codiciado por su valor intrínseco y los grupos de ciberdelincuencia organizada lo reconocen, al llevar a cabo sus actividades ilícitas las realizan desde el anonimato dificultando su persecución. Además, por la gran cantidad de dinero que se ha movido al ciberespacio ha permitido el desarrollo de cibercriminales profesionales y su creciente organización y corporatización (Lusthaus, 2012).

De acuerdo con Posada (2017), la mayoría de los ataques informáticos son llevados a cabo por bandas u organizaciones criminales compuestas por más de tres personas asociadas, quienes incluso emplean mercenarios. Estos ataques suelen ser planeados y realizados de manera autónoma, expansiva y estructurada. Desde una perspectiva en base a su estructura, estas organizaciones criminales pueden tener un mayor grado de autonomía, capacidad de acción y acceso a herramientas tecnologías en distintos niveles.

Estas organizaciones cibercriminales pueden tener estructuras similares a los ejércitos, rígidas y jerárquicas o similares a una empresa criminal que cuenta con autonomía centralizada o descentralizada en diferentes niveles, además de tener la capacidad de contratar mercenarios digitales o servicios de piratería. También se las conoce como “organizaciones virtuales transnacional” debido a su auto legitimación en el ciberespacio y su renovación constante en las

herramientas informáticas. La estructura de las organizaciones cibercriminales transnacionales está relacionada con la comisión de delitos graves y técnicos en el ciberespacio.

Los delitos graves cometidos de manera directa o indirecta por las organizaciones cibercriminales solo son posibles cuando hay una clara distribución de funciones en la cadena delictiva, ya sea horizontal o vertical, guiándose por objetivos específicos, como la obtención de beneficios económicos. Por ello, es posible que la delincuencia organizada convencional participe en gran medida en los delitos cibernéticos que requieren una alta organización y especialización, especialmente aquellos que están motivados por ganancias financieras, como el fraude informático, la falsificación y las infracciones relacionadas con la suplantación de identidad.

Por lo que "los cibercrímenes pueden ser, o bien verdaderos delitos globales realizados mediante canales flexibles e innovadores (correo electrónico, redes sociales, aplicaciones, etc.), o delitos individuales, en ambos casos como conductas deslocalizadas o desubicadas físicamente, que ocurren en la realidad virtual" (Posada, 2017, p. 77). Además, estos grupos de ciberdelincuencia organizada cuentan con la capacidad singular de realizar ataques distribuidos y usar colaboradores conscientes e inconscientes en la realización de los ciberdelitos (Posada, 2019). Estos colaboradores a menudo se convierten en víctimas involuntarias de los ataques, ya que sus sistemas informáticos pueden verse afectados en cualquier parte del mundo.

> Las características tradicionales de la delincuencia organizada, como el uso de la violencia y el control del territorio son difíciles de traducir a la actividad del delito cibernético. Además, las cuestiones de 'gobierno' tradicional en los grupos delictivos organizados, incluyendo la confianza y la aplicación de las normas, pueden no ser fáciles de administrar en un entorno de foros o salas de chat en línea. No obstante, lo que puede hacer un individuo también lo puede hacer una organización –y a menudo puede hacerlo mejor. Internet y las tecnologías relacionadas a este se prestan bien a una coordinación más amplia entre personas en un área dispersa, abriendo posibilidades para asociaciones delictivas tipo enjambre de vida más corta, y a la divergencia con respecto a los modelos tradicionales como los grupos jerárquicos estándar y regionales. (UNODC, 2013, p.51)

La definición de "ciberdelincuencia organizada" es un concepto que no cuenta con un consenso claro, similar a lo que sucede con el de la "ciberdelincuencia". Según el compendio sobre ciberdelincuencia organizada realizado por la Oficina de Naciones Unidas contra la Droga y el Delito (2022), este término se entiende como un delito cibernético, que puede ser facilitado o basado en la cibernética, cometido por un grupo delictivo organizado, según se define en el artículo 2, apartado a), de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional aprobada en 2000, o b) que implique un delito tipificado con arreglo al artículo 5 de la Convención, que penaliza la participación en un grupo delictivo organizado.

En consecuencia, los grupos de ciberdelincuencia organizada son grupos delictivos que cometen delitos cibernéticos. Según lo establecido en el artículo 369 del Código Orgánico Integral Penal, el delito de delincuencia organizada es:

> […] La persona que mediante acuerdo o concertación forme un grupo estructurado de dos o más personas que, de forma permanente o reiterada, financien de cualquier forma, ejerzan el mando o dirección o planifiquen las actividades de una organización delictiva, con el propósito de cometer uno o más delitos sancionados con pena privativa de libertad de más de cinco años, que tenga como objetivo final la obtención de beneficios económicos u otros de orden material, será sancionada con pena privativa de libertad de siete a diez años.
>
> Los demás colaboradores serán sancionados con pena privativa de libertad de cinco a siete años. (COIP, 2014, art. 369)

De acuerdo con el artículo 2, apartado c), de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, un grupo estructurado se define como: “un grupo no formado fortuitamente para la comisión inmediata de un delito y en el que no necesariamente se haya asignado a sus miembros funciones formalmente definidas ni haya continuidad en la condición de miembro o exista una estructura desarrollada” (CNUDOT, 2000, art. 2). Por lo tanto, se puede considerar que un grupo estructurado no tiene que seguir necesariamente una jerarquía. Por lo que es factible considerar que un grupo sin una estructura definida o descentralizado también pueda ser considerado un "grupo estructurado".

Los grupos de ciberdelincuencia organizada deben formarse mediante acuerdo o concertación entre dos o más personas para formar un "grupo estructurado" que actúe en conjunto para el cometimiento de delitos sancionados con pena privativa de libertad de más de cinco años. Además, la persona deberá realizar cualquiera de los siguientes actos: financiar al grupo, ejercer el mando o dirección, o planificar las actividades delictivas. No obstante, el delito de delincuencia organizada exige que cualquiera de los actos mencionados en el tipo penal tenga como característica fundamental la permanencia o reiteración. En consecuencia, el cumplimiento de este requisito implica que la infracción en cuestión solamente puede ser valorada desde la perspectiva de la consumación permanente o delito continuado (Encalada, 2019). La permanencia se refiere a la realización de un acto delictivo que se extiende en el tiempo. Por otro lado, la reiteración hace referencia a la repetición de un mismo acto delictivo con las mismas características típicas en varias ocasiones.

El objetivo de las organizaciones criminales es obtener beneficios económicos u otros de orden material. "Otro beneficio de orden material" no se limita a los beneficios económicos o equivalentes. Además, se debe entender la expresión "otro beneficio de orden material" en un sentido amplio, ya que también puede incluir beneficios personales, como la gratificación sexual, según los "Travaux Préparatoires de las negociaciones para la elaboración de la Convención de Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos" (2022). “Con ello se pretende asegurar que los grupos que intervienen, por ejemplo, en el abuso sexual de niños por motivos no monetarios queden excluidos” (UNODC, 2022, p.9).

Por otro lado, en el caso de la asociación ilícita, normativa que se encuentra ubicada en el artículo 370, capitulo VII, Título IV del Código Orgánico Integral Penal, indica que:

> […] Cuando dos o más personas se asocien con el fin de cometer delitos, sancionados con pena privativa de libertad de menos de cinco años, cada una de ellas será sancionada, por el solo hecho de la asociación, con pena privativa de libertad de tres a cinco años.

De acuerdo con lo establecido en la normativa penal, el elemento objetivo del delito de asociación ilícita no puede presentarse sin que exista una reunión de individuos que constituya una verdadera organización y la intención delictiva común de todos los participantes, razón que los llevo a formas parte de esta y permanecer en está (Resolución Nro. 1453-2012, 2012, CNJ). Lo cual es concordante con lo establecido en el artículo 5 numeral 1, inciso a, literal ii de la Convención de Palermo:

> ii) La conducta de toda persona que, a sabiendas de la finalidad y actividad delictiva general de un grupo delictivo organizado o de su intención de cometer los delitos en cuestión, participe activamente en: a. Actividades ilícitas del grupo delictivo organizado; b. Otras actividades del grupo delictivo organizado, a sabiendas de que su participación contribuirá al logro de la finalidad delictiva antes descrita;

En el caso de la normativa penal interna, el delito de asociación ilícita es sancionado por la mera existencia de una asociación de personas que tengan como finalidad cometer delitos sancionados con pena privativa de libertad de menos de cinco años. Sin embargo, es necesario corroborar que la

> […] reunión de individuos forme una verdadera organización, para lo cual se necesita que sea estable y duradera, y en la cual todos sus participes tengan un rol, una función, un papel dentro de la misma, no basta, por lo mismo, que en los delitos que se han perpetrado o que se planean perpetrar hayan participado varias personas, sino que además haya coordinación y comunicación entre las mismas, lo que permite diferenciar a la asociación ilícita de cualquier otra forma de acto preparatorio o fase previa a la consumación de un delito, o forma de participación intentada en el mismo (Resolución Nro. 1453-2012, 2012, CNJ).

Es por ello, por lo que en un futuro cercano se necesitará una profunda "reestructuración dogmática y político criminal de los delitos de asociación ilícita o de concierto para delinquir en el ciberespacio, que reconozca el cambio de estas organizaciones de un espacio analógico a otro digital" (Posada, 2017, p. 77). La evolución de la ciberdelincuencia organizada representa un reto para las autoridades de hacer cumplir la ley debido a los vacíos normativos, siendo necesario diseñar

una normativa penal que garantice la eficacia de las investigaciones y la limitación del poder punitivo en el ciberespacio.

En efecto, existen diversas diferencias en cuanto a la complejidad estructural y la organización de la ciberdelincuencia organizada con la delincuencia organizada tradicional. Los grupos de ciberdelincuencia organizada presentan vasta gama de estructuras que van desde aquellas que tienen una jerarquía definida, una centralización, roles específicos y lideres reconocibles, hasta aquellas que son redes temporales, sin una estructura clara, laterales, sin una organización fija y descentralizadas. “En algunos casos, la estructura y la organización de los grupos no tenían conexión con personas, sino con el sitio web en el que operaban. Esto se ha observado en sitios de mercados ilícitos en línea tanto en la clearnet (es decir, la web visible) como en la red oscura” (UNODC, 2022, p.16).

Debido a ello McGuire (2012) en su propuesta de clasificación de los grupos del crimen organizado cibernético, identifica seis tipos de estructuras diferentes. Estos grupos pueden evolucionar y cambiar en función del entorno digital en el que operan. La tipología propuesta por McGuire se enfoca en tres tipos principales de grupos:

a) Grupos que operan predominantemente en línea

Se refiere aquellos grupos del crimen organizado cibernético que operan predominantemente en línea. Estos grupos se pueden dividir en dos tipos: enjambres y nodos. La asociación entre los miembros del grupo es principalmente virtual, y la confianza se basa en la reputación que tienen por sus actividades ilícitas en línea.

Enjambres

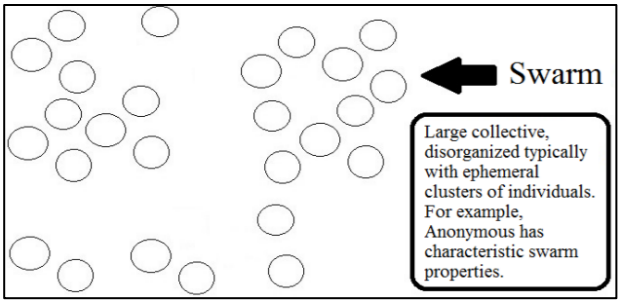

Imagen 6
Grupos del crimen organizado cibernético: enjambre
McGuire, 2012

"Un enjambre puede describirse como la fusión, durante un cierto tiempo, de personas para realizar tareas específicas con el fin de cometer un delito cibernético" (UNODC, 2022, p.17). McGuire (2012) describe a los grupos de enjambre como organizaciones descentralizadas, integradas por un grupo efímero de personas que comparten un propósito en común, pero sin liderazgo ni cadenas de mando. Los enjambres suelen tener un objetivo compartido de llevar a cabo delitos cibernéticos motivados por creencias ideológicas. Los individuos que forman parte de los grupos enjambres generalmente comparten las mismas motivaciones. Como ejemplo de la organización de un enjambre es el grupo hacktivista Anonymous, sin embargo, Anonymous no cuenta con un líder formal, dentro del grupo se presenta un cierto nivel de liderazgo, ya que algunos miembros asumen la iniciativa de planificar, organizar y, en última instancia, tomar decisiones sobre la realización de delitos cibernéticos (UNODC, 2022).

Nodos

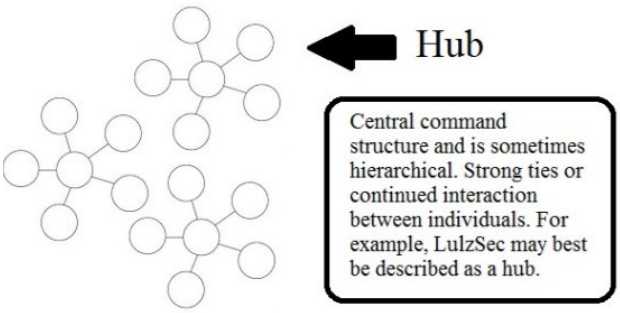

Imagen 7
Grupos del crimen organizado cibernético: centro
McGuire, 2012

Un nodo es un grupo delictivo que consta de una médula central de criminales rodeados de colaboradores adyacentes que cometen actividades delictivas con fines de lucro. A diferencia de los enjambres, los nodos tienen una estructura de mando más definida. Las actividades delictivas que se asocian a este grupo incluyen el phishing, delitos sexuales y las distribución de programas maliciosos, como gusanos informáticos, virus y scareware. Es decir, que cuentan con la existencia de un punto central que actúa como líder de la organización de ciberdelincuentes, que a su vez implica que los asociados periféricos se reúnan para la planificación y distribución de roles (McGuire, 2012).

Un ejemplo de un nodo es Dreamboard:

> […] una empresa delictiva que consistía en un tablero de anuncios en línea que anunciaba y distribuía imágenes de abusos sexuales de niños exclusivamente a sus miembros. Para unirse a Dreamboard, los posibles miembros tenían que proporcionar imágenes de abusos sexuales de niños. Para conservar la condición de miembros de Dreamboard, los miembros tenían que proporcionar continuamente ese tipo de imágenes o de lo contrario se le revocaba el acceso al tablero de anuncios. El acceso de un miembro se revocaba si pasaban 50 días sin que publicara imágenes de abusos sexuales de niños. (UNODC, 2022, p.18)

b) Grupos que operan fuera de línea y en línea

Los grupos que operan fuera de línea y en línea se dedican al cometimiento de delitos en línea y fuera de ella, se describen como grupos “híbridos” que, a su vez, se están subdivididos en agrupados o extendidos.

Híbridos agrupados

El término "híbrido agrupado" hace referencia a una agrupación que lleva a cabo conductas particulares o la utilización de medios específicos para llevar a cabo delitos cibernéticos (UNODC, 2022). Cuenta con una estructura similar a la de los grupos nodo, sin embargo, estos realizan sin

problema delitos en línea y fuera de ella, además de contar con la capacidad para ejecutar actos ilícitos en dos ambientes. Estos grupos puede cometer delitos informáticos en sentido amplio y estricto, utilizan medios tácticos y extraordinarios para realizar los ilícitos. Al igual que los nodos, estos grupos tienen como finalidad la obtención de fines de lucro.

Un ejemplo de grupos híbridos agrupados son aquellos cibercriminales que se dedican a la clonación de tarjetas de crédito en los cajeros automáticos o también conocido como "skimming", y posteriormente usar esos datos para realizar compras en línea o venderlos en mercados negros online de "carding" (McGuire, Soudjn y Zegers, 2012).

Hibrido extendido

Un híbrido extendido es un grupo menos centralizado y más sofisticado que un híbrido agrupado, con un núcleo menos evidente. Está formado por una serie de asociados y subgrupos que realizan diversas actividades delictivas. Sin embargo, cuentan con un nivel de coordinación suficiente para garantizar el éxito de los ilícitos en línea y fuera de ella (McGuire, 2012; Soudjn y Zegers, 2012).

Un ejemplo de híbridos extendidos puede ser:

> […] las comunidades de mercados de la red oscura (como Silk Road, Silk Road 2.0 y Dream Market), que cuentan con administradores y moderadores (que supervisan y dirigen los sitios), vendedores (que venden bienes y servicios ilícitos (estupefacientes sujetos a fiscalización internacional, dinero y documentos falsificados, herramientas y servicios relacionados con la piratería informática, etc.)), compradores (que adquieren bienes y servicios ilícitos) y proveedores (que suministran los bienes a los vendedores), no existe una relación fija y podrían clasificarse como híbridos extendidos. (UNODC, 2022, p.20)

d) Grupos que operan predominantemente fuera de línea

De acuerdo con McGuire (2012) estos grupos operan predominantemente fuera de línea, pero hacen uso de los dispositivos electrónicos o telemáticos para facilitar el cometimiento de actividades ilícitas fuera de ella. Esta clase de grupos de cibercriminales se encuentran evolucionando y actualmente se considera como un factor relevante en el espectro digital a la hora de cometer

actividades ilícitas. Estos grupos suelen tener una estructura jerárquica y están compuestos por organizaciones delictivas tradicionales. Han intentado expandir sus actividades ilícitas en línea, como la extorsión, la prostitución y el tráfico de personas.

Jerarquías

Según McGuire (2012), los grupos cibercriminales con jerarquías comparten características con la delincuencia organizada tradicional. Villapando (2008) (citado por Mancilla, 2014) describe dos modelos de crimen organizado: el modelo del padrino, donde el poder se concentra en una familia o pequeño grupo que controla un territorio o servicio específico de manera jerárquica, y el modelo de empresa, que involucra una distribución de responsabilidades internas y jerarquías administrativas similares a las operaciones de gestión empresarial. El crimen organizado ha aprovechado la proliferación de sistemas informáticos para ampliar sus actividades ilícitas y obtener beneficios económicos. Los grupos del crimen organizado utilizan Internet para la coordinación de delitos comunes, como la venta de sustancias sujetas a fiscalización o la extorsión. Además, con la aparición del ransomware, se ha evidenciado una participación de grupos del crimen organizado, con la finalidad de cifrar información mediante el uso de software malicioso y exigir un rescate para evitar la divulgación o eliminación de esta (EUROPOL, 2020).

Agregados

Los grupos de esta naturaleza carecen de una estructura definida, son efímeros y a menudo no tienen un objetivo claro. Utilizan dispositivos electrónicos o informáticos de manera ad hoc, aunque pueden causar daños. Durante doce días en 2019, se llevaron a cabo manifestaciones en Quito que causaron perjuicios patrimoniales e inestabilidad del Estado. Las tecnologías desempeñaron un papel importante en la generación de disturbios públicos y en la coordinación entre pandillas para cometer delitos (Cubby, 2012; McNeilage, 2012).

1.3. Redes anónimas y su relación con el cibercrimen

El internet está formado por redes abiertas, públicas y privadas. Al acceder a una aplicación en una red abierta, la identidad del usuario queda expuesta, lo que permite que terceros rastreen su actividad en línea (Acosta, 2019). Por lo tanto, los sitios web que utilizan IRC (Internet Relay Chat), así como los contenidos a los que se accede, pueden ser identificados o supervisados. Aunque existe la posibilidad de que los usuarios utilicen técnicas o software para anonimizar sus datos, lo que implica eliminar cualquier información que pueda identificar al usuario.

Aunque no es posible obtener un anonimato completo en las redes anónimas, proporcionan al usuario más opciones para ocultar sus actividades en línea. La información y el contenido que se comparten a través de estas redes están cifrados y, por lo tanto, el usuario puede ser anónimo, al igual que sus acciones. A menudo se cree que las redes anónimas se utilizan únicamente para actividades delictivas, pero también pueden ser utilizadas para proteger la libertad de expresión en gobiernos autoritarios o disidentes (INTERPOL, 2017). Según el Proyecto Tor (2013), los usuarios usan esta red para evitar el rastreo de sitios web hacia ellos o sus familiares, o para acceder a sitios de noticias o servicios de mensajería que son bloqueados por sus proveedores de Internet locales.

Las empresas que escanean la web y proporcionan motores de búsqueda, como Google, Bing, Yandex y DuckDuckGo, utilizan rastreadores informáticos especializados para indexar el contenido y hacerlo fácilmente localizable para los usuarios de Internet. Sin embargo, estas herramientas tienen limitaciones en cuanto a la exploración de datos para su indexación. Por ejemplo, no pueden explorar datos dentro de redes anónimas, páginas con acceso restringido y áreas privadas de Internet. Es importante tener en cuenta que los motores de búsqueda estándar no

indexan estos tipos de sitios web, lo que hace que los datos dentro de ese entorno sean difíciles de identificar o descubrir a través de procesos convencionales (UNODC, 2021).

Las redes anónimas no son ilegales, ya que almacenan información en línea que los usuarios no quieren compartir públicamente. Este tipo de información incluye material académico de universidades de carácter reservado, datos restringidos por la policía, secretos industriales de empresas, historiales médicos de hospitales, entre otros (INTERPOL, 2020). Por lo general, este tipo de información requiere una cuenta y una credencial para acceder nuevamente, y se encuentra en lo que se conoce como la darknet.

En el Ecuador las redes anónimas no son ilegales, al igual que en la mayoría de las jurisdicciones, la darknet - el subconjunto de la web superficial- facilita las actividades ilícitas. Para acceder a la darknet se requiere de un protocolo específico. Entre ellos se encuentran los siguientes:

- Freenet
- Proyecto Internet Invisible (IP2)
- Loopix
- The Onion Router (TOR)
- DNS descentralizado o Blockchain (B-DNS) - Peername.com registrador de nombres de dominio de Namecoin, Emercoin, NTX y ethereum.
- DNS alternativos

Las redes anónimas son independientes entre sí y no están vinculadas. Cada red anónima requiere un programa específico para acceder a ella. Por ejemplo, para acceder a Freenet se necesita un programa, y para acceder a Loopix se requiere otro. Para ingresar a estas redes, los usuarios deben acceder a Internet a través de un ISP y ejecutar el programa correspondiente de la red anónima a la que quieren ingresar. El protocolo más comúnmente utilizado por los delincuentes para acceder y establecer servicios ocultos o mercados en la darknet es TOR.

Una vez que los usuarios acceden a una red anónima, pueden utilizar aplicaciones como lo harían en una red de Internet abierta. Por ejemplo, podrían conectarse a un IRC y utilizar sitios web o aplicaciones a través de ese programa. Sin embargo, las aplicaciones en una red anónima no son accesibles desde fuera de ese entorno específico. Para acceder a ese entorno, los usuarios necesitan obtener el permiso del operador de la red o la aprobación de un usuario existente.

Por lo que a medida que los ciberdelincuentes utilizan cada vez más la darknet, se ha convertido rápidamente en uno de los temas más discutidos por miembros de la fuerza pública y justicia penal. Este interés sin precedentes ha llevado a las fuerzas del orden a crear mecanismos y procesos para investigar la criminalidad que ocurre en la darknet. Sin embargo, hay una participación limitada e inconsistente a nivel global, lo que reduce la cooperación internacional y aumenta las oportunidades del cibercrimen.

Es así como el interés público en la darknet ha aumentado en los últimos años, pues su ecosistema de anonimato ha evolucionado de ser un canal de comunicación para actores de privacidad a un mercado global con una amplia variedad de productos y servicios disponibles para su compra (UNODC, 2021). Además, la darknet funciona como plataforma para una gran cantidad de foros de discusión que abordan diversos temas, y que a veces están organizados por nacionalidad, idioma o tipo específico de delitos como el fraude de tarjetas de crédito, el trading interno, el tráfico de drogas, el tráfico de armas y el crimen como servicio o “crime -as- a-Service” (CaaS).

Como consecuencia del creciente uso de la tecnología de anonimización, los mercados ilícitos de darknet se han vuelto más accesibles y populares. Después de la introducción de Bitcoin en 2009, se adoptó rápidamente como método de pago en los mercados oscuros. En particular, en 2011, el mercado de Silk Road, un sitio web de cebolla que proporcionaba una plataforma para

comprar y vender productos ilegales (principalmente drogas), comenzó a operar dentro de la red Tor utilizando Bitcoin como su método de pago principal (aunque hoy en día el uso de monedas privadas, como Monero y Ethereum, está aumentando). Silk Road fue la primera vez que se combinaron estas tecnologías para permitir que un mercado en línea de productos ilegales creciera significativamente (INTERPOL, 2019).

Estos mercados ilícitos no han inventado nuevas tecnologías, sino que han combinado diversas innovaciones que generan nuevos beneficios tanto para vendedores como para compradores. Las criptomonedas, debido a su amplia anonimidad, se han convertido en el medio para financiar la ciberdelincuencia en la darknet. El número de mercados activos en la darknet ha pasado de uno (Silk Road) en 2011 a 118 en 2019. Estos mercados compiten entre sí y la mayoría de los usuarios solo utilizan el mercado más popular ya que es menos probable que sea una estafa (UNODC, 2020). Estos mercados funcionan como sitios web de comercio electrónico tradicionales, excepto que generalmente son bienes y servicios ilícitos los que se compran y venden

De acuerdo con la Oficina de las Naciones Unidas contra la Droga y el Delito (2020), estos mercados ilícitos cuentan con cuatro componentes para operar:

1. Una plataforma anónima y resistente a la censura para operar, por ejemplo, un sitio web de cebolla.
2. Un sistema monetario en línea (semi) anónimo, es decir, Bitcoin.
3. Un sistema de pago de garantía (contabilidad de garantía interna).
4. Reputación y retroalimentación (métrica de reputación transparente). (UNODC, 2020, p.20)

En definitiva, el uso de redes anónimas y el cibercrimen se encuentran estrechamente relacionadas por diversos motivos, siendo el principal el anonimato que ofrecen estas plataformas. Si bien es cierto que las redes anónimas se encuentran amparas por el derecho a la privacidad y a la libertad de expresión, han sido mal utilizadas por los ciberdelincuentes para llevar a cabo actividades ilegales. Es importante adecuar las medidas necesarias por parte de los Estados para

combatir el cibercrimen, pero también se debe reconocer que estas redes no son inherentemente malas y pueden ser usadas de manera responsable y dentro de los parámetros legales.

Capítulo II. Técnicas especiales de investigación: El agente encubierto informático

2.1. Concepto de técnicas especiales de investigación y agente encubierto informático

La ciberdelincuencia se distingue de la delincuencia tradicional por operar en el anonimato y tomar mayores precauciones para evitar alertar a las fuerzas de seguridad durante la preparación y ejecución de sus actividades. Debido a esto, los métodos de investigación tradicionales a menudo resultan ineficaces ante las estructuras empleadas por el cibercrimen organizado y la habilidad de sus actores. Para abordar esta problemática, se utilizan técnicas especiales de investigación que permiten la infiltración adecuada en las organizaciones criminales.

No existe un concepto universalmente aceptado en relación al concepto de técnicas especiales de investigación, es por ello por lo que la doctrina penal se ha encargado de definir como:

> […] actividades de las autoridades desarrolladas desde la clandestinidad para someter en diversas formas de crimen y que comportan un riesgo de la seguridad no solo del individuo que participa en tal actividad, sino de la sociedad en cuento a la libertad de ambulatoria y la privacidad. (Montoya, 1998, p.352)

Tal como hace mención su nombre "técnicas especiales de investigación", son especiales, lo que implica que su uso sea excepcional, debido a que puede afectar de cierta manera los derechos humanos de los sujetos investigados, por lo que se debe valorar dicha injerencia para evitar excesos o arbitrariedades por parte del Estado. Sin embargo, son de suma importancia para la recopilación de información sobre las actividades de los ciberdelincuentes o de grupos del crimen organizado. La elección de la técnica más eficaz dependerá de las necesidades operativas para recopilar información del delito.

En el derecho interno, las técnicas especiales de investigación se encuentran tipificadas en la sección tercera del libro segundo del Código Orgánico Integral Penal, de esta manera se establecen

distintas formas de investigaciones especiales como: "operaciones encubiertas, entregas vigiladas o controladas, cooperación eficaz, informantes" (COIP, 2014). En el mismo sentido, a nivel internacional, el artículo 20 de la Convención de Naciones Unidas contra la Delincuencia Organizada Transnacional alienta, en medida de lo posible a cada Estado, el uso adecuado de las técnicas especiales de investigación con la finalidad de combatir de manera eficaz a la delincuencia organizada. El reconocimiento de las técnicas especiales de investigación a nivel internacional surgió de una reunión de expertos en Varsovia en febrero de 1998, en donde ya incluía disposiciones, basadas en parte en el artículo de la Convención de Viena de 1998 sobre entrega vigilada o controlada, vigilancia electrónica y operaciones encubiertas (McClean, 2007).

Por lo tanto, el uso de las técnicas especiales de investigación se encuentra amparado a nivel internacional e interno. Además, que uno de los deberes del Estado ecuatoriano es "(…) garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral a vivir en una sociedad democrática y libre de corrupción. (CRE, 2008, art. 3 numeral 8) En cuanto a la noción del término de seguridad este ha ido evolucionando en relación al estado de derechos y justicia; "así la idea de seguridad estadocéntrica ha sido remplazada por una seguridad basada en las personas; entendida esta como seguridad humana" (Corte Constitucional del Ecuador, 2021, sentencia No. CCE-13-14-IN/21, p. 10), lo cual resulta concordante con lo señalado en el artículo 393 de la Constitución de la República del Ecuador:

> […] El Estado garantizará la seguridad humana a través de políticas y acciones integradas, para asegurar la convivencia pacífica de las personas, promover una cultura de paz y prevenir las formas de violencia y discriminación y la comisión de infracciones y delitos. La planificación y aplicación de estas políticas se encargará a órganos especializados en los diferentes niveles de gobierno. (CRE, 2008, art. 393)

Por lo tanto, el Estado se encargará de garantizar la "seguridad humana" para lograr objetivos como la convivencia pacífica, la cultura de paz y la prevención de formas de violencia,

discriminación y comisión de delitos. Para ello se implementará políticas públicas, que se encuentran instrumentadas de diversas formas, incluyendo el desarrollo normativo (Corte Constitucional, 2021, sentencia No. CCE-13-14-IN/21). Este enfoque polémico se encuentra correlacionado con el "derecho penal de la seguridad", caracterizado principalmente por la adopción de medidas y políticas criminales que permitan prevenir y combatir la delincuencia, el terrorismo, los ciberdelitos y otras amenazas a la seguridad pública, incluso si se tiene que restringir derechos específicos y garantías procesales de los investigados.

Como fundamento del derecho penal de la seguridad se tiene la idea de que la seguridad pública es un derecho fundamental que debe ser garantizado por el Estado, y que la prevención, investigación y represión de los delitos requieren de medidas efectivas y contundentes, incluso a costa de una mayor intervención y vigilancia estatal, o la limitación de ciertos derechos fundamentales. Esta idea ha sido objeto de debate y controversias, específicamente por el impacto que puede tener estas medidas en los derechos humanos, algunos críticos señalan que este enfoque puede desbordarse y convertirse en un Estado Policial en donde se vulnere derechos como la privacidad, la protección de los datos personales, la no autoincriminación, la libertad de expresión, entre otros.

Otros autores, consideran que el derecho penal puede ser utilizado legítimamente para proteger la seguridad y prevenir el peligro, y este puede adaptarse a las necesidades sociales actuales sin comprometer el sistema de garantías. Esta perspectiva se centra en la consolidación de la seguridad como un valor fundamental y considera que el derecho penal puede ser una herramienta útil para lograr este objetivo (Mendoza, 2001).

Por lo tanto, se debe resaltar que el más alto deber del Estado ecuatoriano, de acuerdo con el artículo 11 numeral 9 de la Constitución del Ecuador consiste:

> […] respetar y hacer respetar los derechos garantizados en la Constitución. El Estado, sus delegatarios, concesionarios y toda persona que actúe en ejercicio de una potestad pública, estarán obligados a reparar las violaciones a los derechos de los particulares por la falta o deficiencia en la prestación de los servicios públicos, o por las acciones u omisiones de sus funcionarias y funcionarios, y empleadas y empleados públicos en el desempeño de sus cargos. El Estado ejercerá de forma inmediata el derecho de repetición en contra de las personas responsables del daño producido, sin perjuicio de las responsabilidades civiles, penales y administrativas. El Estado será responsable por detención arbitraria, error judicial, retardo injustificado o inadecuada administración de justicia, violación del derecho a la tutela judicial efectiva, y por las violaciones de los principios y reglas del debido proceso. Cuando una sentencia condenatoria sea reformada o revocada, el Estado reparará a la persona que haya sufrido pena como resultado de tal sentencia y, declarada la responsabilidad por tales actos de servidoras o servidores públicos, administrativos o judiciales, se repetirá en contra de ellos. (CRE ,2008, art. 11 numeral 9)

Entonces, en general, el marco normativo nacional e internacional permite al Estado ecuatoriano adoptar medidas legislativas para la lucha contra el cibercrimen y el crimen organizado, con el objetivo de garantizar la seguridad ciudadana. Para lograr este objetivo, se debe considerar el uso de técnicas especiales de investigación como medio más eficaz de investigación penal, sin que ello implique un exceso o abuso por parte del Estado, ya que esto estaría sujeto a las responsabilidades civiles, administrativas o penales previstas en el ordenamiento jurídico.

Considerando que, en la actualidad, los mecanismos de investigación penal no satisfacen las necesidades de los miembros de la fuerza pública para abordar el creciente fenómeno de los ciberdelitos, por lo tanto, es necesario modernizar el proceso penal para enfrentar este desafío. Sin embargo, cualquier modernización debe cumplir con parámetros de constitucionalidad y la protección de los derechos fundamentales de los sospechosos. Es así, que lo ideal sería encontrar un punto de equilibrio entre el respeto de los derechos humanos de las personas investigadas y la seguridad humana como obligación del Estado.

En ciertas ocasiones, el Estado cede a la presión de los medios de comunicación por el clamor ciudadano de seguridad, sin considerar en lo mínimo lo técnico ni las desventajas de aumentar el poder punitivo del Estado. El objetivo principal en estos casos es aplicar el ius puniendi a cualquier costo, sin tener en cuenta los parámetros de constitucionalidad. Adoptar esta postura puede llevar

a que los postulados del derecho penal liberal sean desvirtuados y pueda ceder ante un Estado Policial, violentando el principio de mínima intervención penal y las garantías del debido proceso.

En este sentido, explica el jurista argentino Raúl Zaffaroni (2008) que:

> Las garantías penales y procesales penales no son producto de un capricho, sino el resultado de la experiencia de la humanidad acumulada en casi un milenio, en lucha constante contra el ejercicio inquisitorial del poder punitivo, propio de todas las invocaciones de emergencias conocidas en todos estos siglos, en que el poder punitivo descontrolado emprendiendo empresas genocidas causó más muertes y dolor que las propias guerras. (p.14)

Es por ello, que, en la lucha contra el cibercrimen y la ciberdelincuencia organizada, la eficacia del proceso penal y las garantías al debido proceso deben buscar una armonía para coexistir en un Estado de Derecho. La búsqueda de esta coexistencia representa uno de los grandes desafíos del proceso penal en las sociedades postindustriales. Actualmente, el debate se centra en la colisión de dos intereses; por un lado, la obligación del Estado de garantizar la seguridad pública mediante el desarrollo normativo y la eficacia en las investigaciones criminales del siglo XXI; por otro, el respeto estricto de los derechos y garantías fundamentales de los sospechosos o imputados en el proceso penal para no convertirse en un Estado Policial.

La lucha contra la cibercriminalidad ha planteado la preocupación en la dogmática penal por los posibles abusos o excesos en la actuación de la potestad castigadora del Estado, generando la necesidad de que el derecho procesal penal moderno considere los retos que existen en la detección y recolección de información en el ciberespacio. Sin embargo, no se debe permitir un régimen de doble vía en el cual se establezcan normas más severas para los ciberdelincuentes y el crimen organizado transnacional. Esto último podría resultar en la legitimación del los postulados del derecho penal del enemigo, desarrollando normas diferenciadas para un cierto sector de la sociedad y para el enemigo.

En este sentido, para que el ius puniendi mantenga un equilibrio en un estado de derecho, se debe considerar tres principios: la eficacia del proceso penal en la actualidad, la búsqueda de la verdad material de los hechos y la celeridad en las investigaciones criminales. No obstante, en la búsqueda de la eficacia, no se puede violar los derechos fundamentales y las garantías del debido proceso de los sospechosos. Por lo tanto, para lograr una verdadera eficiencia en el proceso penal, se debe reconocer la importancia de garantizar el debido proceso durante la investigación criminal. En sentido estricto, la misión del derecho procesal penal en un Estado de Derechos en la actualidad es hallar nuevas herramientas de investigación criminal que permitan la ejecución del derecho penal procesal penal y el respeto a los derechos humanos de los sospechosos o imputados.

Es por ello por lo que es imprescindible tener en cuenta que el desempeño óptimo del proceso penal en la esfera de la lucha contra la ciberdelincuencia y el crimen organizado cibernético se encuentra ligado a la asunción de posturas renovadas por parte de los funcionarios judiciales, además de la incorporación de nuevas técnicas de investigación (Baltazar, 2004). En consecuencia, resulta esencial instituir un punto de equilibrio entre las fuerzas en conflicto en la lucha contra la ciberdelincuencia, sin incurrir en un abuso instrumentalizado de las garantías del debido proceso y los derechos fundamentales.

De esa manera, en la actualidad, el Código Orgánico Integral Penal establece en su Capítulo IV las "Actuaciones y Técnicas Especiales de Investigación". En la Sección Tercera de dicho capítulo, se describen las técnicas especiales de investigación, entre las cuales se encuentra la utilización de operaciones encubiertas en espacios físicos e informáticos. En este sentido, el artículo 483 del COIP señala que esta técnica especial de investigación es excepcional y está bajo la dirección de una unidad especializada de la Fiscalía General del Estado. Dicha unidad es la encargada de planificar y ejecutar la operación encubierta con el personal del Sistema Especializado Integral de

Investigación, de Medicina Legal y Ciencias Forenses. El objetivo de la operación encubierta es autorizar a los agentes a infiltrarse en organizaciones o agrupaciones delictivas, ocultando su identidad oficial, con el propósito de identificar a los participantes, recopilar información, elementos de prueba y evidencia útil para los fines de la investigación (Corte Constitucional del Ecuador, 2021, sentencia No. CCE-13-14-IN/21).

En esta línea, la Corte Constitucional del Ecuador ha definido a la figura del agente encubierto como:

> […] aquella persona que, integrada de ordinario, dentro de la estructura orgánica de los servicios policiales o de acuerdo con éstos, se introduce, ocultando su verdadera identidad, dentro de una organización criminal, con la finalidad de recabar información de esta, y proceder, en consecuencia, a su desarticulación. (Corte Constitucional del Ecuador, 2021, sentencia No. CCE-13-14-IN/21)

"El recurso a un agente encubierto forma parte de la técnica policial de investigación denominada infiltración" (Carou, 2021, p. 829). De acuerdo con Gascón Inchauisti (2019) menciona que la infiltración es:

> […] la acción de aquel que, para obtener información que no es de acceso general y que le es necesaria para un propósito concreto oculta tanto su identidad real como sus intenciones y, bien directamente bien a través de un tercero, entre en contacto con las personas aparentemente susceptibles de suministrársela, estableciendo con ellas una falsa relación de confianza que, con el transcurso del tiempo, le permita obtener información deseada (citado por Carou, 2021, p. 829).

Según Zafra Espinosa de los Monteros (2010) la diferencia entre agente encubierto e infiltración policial radica en que "la infiltración policial, debemos configurarla como la técnica de investigación, mientras que el agente encubierto es el medio por el que se hace efectiva la infiltración policial" (p.76). El uso de los términos "agente encubierto" y "agente infiltrado" como sinónimos es un error y evidencia una falta de conocimiento jurídico. Estos términos se refieren a dos modalidades de investigación diferentes en el ámbito del derecho penal. Mientras que el agente encubierto es el instrumento al servicio de una técnica de investigación (Rodríguez, 2012), la infiltración es la acción de aquel que, para obtener información que no es de acceso general y que

le es necesaria para un propósito en concreto, oculta su identidad real como sus intenciones (Inchausti, 2001). “Así pues el reconocimiento legislativo del agente encubierto, en cuanto instrumento propio de la infiltración policial, supone a la postre, el reconocimiento legal de la propia técnica de infiltración” (Carou, 2021, p. 830).

Ahora bien, la creciente dependencia de las tecnologías de la información y la comunicación a nivel global, particularmente en relación con la delincuencia organizada transnacional, ha llevado a que las agencias encargadas de hacer cumplir la ley hayan tenido que adaptar sus estrategias de investigación y vigilancia a un contexto digital. Una de esas nuevas técnicas de investigación digital son el uso de agentes encubiertos informáticos, que permiten a las autoridades investigar y recopilar pruebas con mayor facilidad en relación con los delitos cometidos en línea.

Por lo tanto, es necesario replantear el derecho penal en virtud de las características inherentes a la ciberdelincuencia, además del desarrollo de ilícitos en los entornos digitales. La capacidad de mutación propia de esta forma de delincuencia plantea un desafío normativo y político criminal. Históricamente, los sistemas jurídicos fueron diseñados para combatir a la delincuencia física, que se limitaba a un espacio geográfico determinado. Es así como en el ordenamiento jurídico ecuatoriano, la tipificación de conductas relacionadas con la ciberdelincuencia y los medios de investigación destinados a combatir el cibercrimen se encuentran limitados. Siendo necesario de esta manera reformular la política criminal para afrontar los retos del siglo XXI, sin menoscabo de los principios fundamentales del derecho penal -como el de legalidad, mínima intervención o seguridad jurídica-, sino dotando a los operadores de justicia de las herramientas necesarias que, en el marco del respeto a los derechos y garantías fundamentales, les permitan hacer frente a una nueva realidad digital.

Con respecto a la figura del agente encubierto informático esta se asemeja en sus funciones al agente encubierto convencional, sin embargo, difiere en la forma en que realiza su infiltración, ya que el agente encubierto informático se desenvuelve en línea, específicamente en canales cerrados de comunicación donde terceros ajenos a la conversación no podrían ingresar. Por consiguiente, se podría definir al agente encubierto informático como:

> […] un empleado o funcionario público que, voluntariamente, y por decisión de una autoridad judicial, se infiltra en la red con el fin de obtener información sobre autores de determinadas prácticas ilícitas producidas a través de la red y que causen una gran repulsa y alarma a nivel social. Su función consistiría en la ocultación de la verdadera identidad policial, con el fin de establecer una relación de confianza que permita al agente integrarse durante un periodo de tiempo prolongado en el mundo en el que los "ciberdelincuentes" actúan con la finalidad primordial, igualmente oculta, de obtener información necesaria para desenmascarar a los supuestos criminales. (Bueno de Mata, 2011, p.115)

El agente encubierto informático es una técnica especial de investigación enfocada en perseguir delitos cometidos en línea y en el crimen organizado cibernético, los cuales se valen del anonimato de la red para escapar de las barreras ordinarias. Esta medida de investigación es particularmente adecuada para la investigación de delitos con una importante dimensión informática. La creciente aparición de mercados negros en línea ha dotado a los ciberdelincuentes de herramientas para eludir los controles y medidas de prevención convencionales.

Pues, la persecución de cibercriminales presenta una dificultad considerable debido a las diversas opciones de anonimato que ofrece Internet. Por lo tanto, la infiltración del agente encubierto informático se considera una medida efectiva para combatir la delincuencia organizada en línea, dado el fracaso de los métodos de investigación tradicionales para abordar este problema criminológico. De acuerdo con la autora Carou García (2021):

> […] el universo virtual se ha convertido en el gran espacio de socialización de estos tiempos, por lo cual la aplicación de mecanismos de ingeniería social -sobre los que se asienta la actuación del agente encubierto-enfocados a la averiguación de las acciones delictivas en la red resultan especialmente idóneos para dicha finalidad. (p.838)

El agente encubierto informático utiliza el engaño para obtener información relevante para el proceso penal, lo cual plantea una colisión entre dos valores fundamentales. Por un lado, "la licitud de los medios utilizados por un Estado de Derecho y por la otra, la eficacia para combatir un delito que tan graves daños ocasiona y tanta repulsa tiene por parte de la sociedad" (Bueno de Mata, 2011, p.302). Investigar la ciberdelincuencia que opera en canales cerrados de comunicación no es tarea sencilla para los agentes de control. Los mercados ilícitos en línea se prestan para el almacenamiento masivo de material ilícito sobre abuso sexual a menores, al cual solo se puede acceder con la confianza de los usuarios de la red. Por lo tanto, recolectar indicios se vuelve complicado, especialmente cuando se debe identificar al humano detrás del teclado.

De acuerdo con el maestro Federico Bueno de Mata (2019), en su obra diligencias de investigación penal en la cuarta revolución industrial, señala que:

> La justificación del engaño usado por el agente encubierto radica en una cuestión de política criminal, que llega a justificar las consecuencia devastadoras que su utilización implica. La solución viene dada por una ponderación de valores, en el que se acaba por dar preponderancia al valor "eficacia", en el sentido que, si se quiere luchar eficazmente con este delito tan oculto, la mejor manera y la opción idónea es infiltrar a la persona de esta manera para llegar a una situación más favorable para la sociedad. Estamos eligiendo así una solución que reporta más seguridad y bienestar al conjunto de la sociedad y que logra la justicia, objetivo capital en un Estado de Derecho. (p.114)

Finalmente, la figura del agente encubierto informático se incorporó en el Código Orgánico Integral Penal mediante la Ley Orgánica Reformatoria a varios cuerpos legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral, publicada en el Suplemento del Registro Oficial No. 279 el 29 de marzo del 2023, en la que se señala a esta técnica especial de investigación como:

> […] La o el fiscal podrá autorizar al personal del Sistema Especializado Integral de Investigación de Medicina Legal y Ciencias Forenses, realizar tareas de gestión investigativas ocultando su verdadera identidad, asumiendo identidad supuesta, para lo cual deberán realizar patrullajes o acciones digitales en el ciberespacio, penetrándose e infiltrándose en plataformas informáticas como foros, grupos de comunicación o fuentes cerradas de información o comunicación, con la finalidad de hacer seguimiento de personas, vigilar cosas, realizar compras controladas y/o descubrir, investigar o esclarecer

> hechos delictivos cometidos o que puedan cometerse con el uso o en contra de las tecnologías de la información y comunicación, esto es ciberdelitos puros o replicas o cualquier otro tipo de delito. En el desarrollo de sus actividades, podrá intercambiar, enviar de manera directa archivos, ficheros con contenido ilícito o aplicar técnicas para preservar y descifrar información recolectada que sea útil para la investigación. Además, podrá obtener imágenes y realizar grabaciones en audio o video, de las conversaciones que podría llegar a mantener con el o los investigados, dependiendo de la naturaleza y modus operandi de la organización, con la utilización de cualquier medio tecnológico, en cualquier lugar, para lo cual el fiscal previamente obtendrá la respectiva autorización judicial. (COIP.2023, art. 483.1)

El COIP no ofrece una definición propia de lo que se entiende por agente encubierto informático. Pues bien, de acuerdo con la normativa vigente y la doctrina predominante en el tema se deduce que la figura del agente encubierto informático, de modo general, es un funcionario perteneciente al Sistema Especializado Integral de Investigación de Medicina Legal y Ciencias Forenses que cuenta con habilidades de programación, así como con conocimiento amplio y profundo sobre sistemas informáticos, que se infiltra voluntariamente en canales cerrados de comunicación por disposición de la autoridad competente, en el caso ecuatoriano por parte de la Fiscalía General del Estado, con la finalidad de hacer seguimientos de personas, vigilar, realizar comprar controladas y/o investigar o esclarecer hechos delictivos cometidos o que pueden cometerse con el uso o en contra de las tecnologías de la información y comunicación, para lo cual ocultara su verdadera identidad y asumirá una identidad supuesta en el ciberespacio. Asimismo, podrá enviar archivos o ficheros con contenido ilegal directamente a través de una autorización especial, ya sea dentro de la misma resolución judicial con una justificación separada y adecuada, o en otra resolución judicial diferente.

Por ello, el uso de agentes encubiertos informáticos es un diligencia de investigación criminal altamente eficaz para obtener elementos de convicción y además permitiría identificar a los responsables de los delitos cibernéticos contra sistemas informáticos o perpetrados por seres humanos a través de los sistemas informáticos. Esto se debe a que, al infiltrarse de manera secreta

en canales de comunicación cerrados, el agente puede presenciar directamente los delitos cometidos por los autores y sus cómplices. Es importante considerar que esta técnica no es ordinaria, sino que es excepcional y su uso debe cumplir con los principios de necesidad, idoneidad y proporcionalidad.

Al respecto de las operaciones encubiertas online es preciso indicar que:

> […] después de capacitar a agentes especiales que puedan hablar, y dado los recursos para pasar suficientes horas en línea durante un período prolongado de tiempo, hemos descubierto que casi cualquier empresa ciberdelincuente comenzará a confiar en nosotros, a pesar de que nunca nos conoció cara a cara. También aprendimos que los métodos de comunicación utilizados por estos delincuentes son, para ellos, también una salida social. Tan a menudo como hablan de malware, delitos y productos para la venta, hablan de sus familias, sus novias, sus vacaciones y sus automóviles. Después de un tiempo, los miembros de estos foros se hacen amigos. De ahí proviene la confianza intrínseca. Cuando alguien ingresa por primera vez como miembro nuevo, se lo considera un policía potencial; un mes después, son menos policías; seis meses después, son amigos; Un año después... (Chabinsky, 2010)

En el funcionamiento de la figura investigativa del agente encubierto informático, una de las dificultades radica en la falta de una lista explícita de características que deba poseer dicho agente. Para subsanar esta situación, Del Pozo Pérez propone una serie de cualidades relevantes que se deben considerar al otorgar el cargo, como habilidades psicológicas (por ejemplo, empatía, confidencialidad, discreción o capacidad para tomar decisiones de forma autónoma) y sólidos conocimientos informáticos que vayan más allá del nivel de usuario común (Bueno de Mata, 2019). Para ser considerado un agente encubierto informático idóneo, se propone que la persona debe formar parte de la Unidad de Ciberdelitos de la Policía Nacional del Ecuador, que pertenece al Sistema Especializado Integral de Investigación de Medicina Legal y Ciencias Forenses.

En cuanto a las facultades, en el artículo 483.1 del COIP determina las potestades del agente encubierto informático, entre las cuales se destaca el intercambio, envío de manera directa de archivos o ficheros con contenido ilícito (COIP,2014). Sin embargo, esta facultad ha sido criticada por un sector de la doctrina penal donde se cuestiona, ¿a qué se refiere con ficheros con contenido

ilícito?, ¿cómo recuperarlos una vez que ha sido enviado?, es por ello por lo que De la Rosa Cortina (2011) señala lo siguiente:

> […] la policía podría, en el curso de una investigación y con la cobertura de la regulación del agente encubierto, con respeto al PRINCIPIO DE PROPORCIONALIDAD, difundir material pornográfico si ello es necesario, por ejemplo, para infiltrarse en un grupo de pederastas, previa autorización al respecto». Sin embargo, por archivo ilícito cabe entender también el envío de spyware, troyanos, etc., lo que tendrá una repercusión diferente en los derechos fundamentales del sujeto investigado. (p. 143)

Sin embargo, es importante señalar que la autorización para llevar a cabo una investigación no significa que se tenga la libertad de actuar de manera indiscriminada, sino que debe haber una relación lógica entre la investigación y las medidas adoptadas, las cuales deben ser proporcionales y no deben provocar la comisión de un delito. Actualmente, no existe una regulación tácita que cumpla con el principio de legalidad en cuanto al uso de "troyanos", "spyware" o "keyloggers", por lo que esta opción no es viable. Cualquier elemento probatorio obtenida de esta manera sería contraria a la Constitución de la República del Ecuador y constituiría una prueba ilícita, además de violar de manera abusiva el derecho a la intimidad personal de los sospechosos.

De igual manera se establece que el agente encubierto informático en el transcurso de la investigación podrá realizar “compras controladas” con la finalidad de confirmar o descartar la existencia de una actividad delictiva presuntamente cometida por una persona. Esta técnica complementaria requiere de la figura del agente encubierto quienes actúan únicamente después de obtener información precisa de que la persona objeto de la investigación está involucrada en una actividad delictiva. Su acción se limita a corroborar esta información, pero jamás en provocar el delito. Para lo cual, es necesario una autorización complementaria a la medida principal por parte de un Juez de Garantías Penales por petición de la Fiscalía General del Estado. Las compras controladas deben estar sujetas a límites rigurosos para evitar la provocación del delito.

Por lo tanto, el uso de agentes encubiertos informáticos no está exento de controversia. En muchos casos, los agentes encubiertos deben operar entre la legalidad y la ilegalidad, lo que puede resultar en desafíos éticos y legales. Por ejemplo, los agentes encubiertos pueden ser acusados de "provocar" delitos que, de otro modo, no se habrían cometido. Además, la posibilidad de que un agente encubierto cometa delitos mientras está en línea, como la descarga de archivos ilegales, plantea desafíos éticos y legales.

Para ello, es importante que la utilización de agentes encubiertos informáticos esté sujeta a límites y salvaguardas adecuadas. Las autoridades encargadas de hacer cumplir la ley deben seguir protocolos claros para garantizar que la utilización de agentes encubiertos informáticos sea proporcional y necesaria. Además, se deben establecer medidas para proteger los derechos y las libertades individuales, como el derecho a la privacidad en línea, la protección de los datos personales, la no autoincriminación y la autodeterminación informativa.

En conclusión, el agente encubierto informático es una herramienta efectiva para combatir los delitos cibernéticos en la actualidad. Si se utiliza adecuadamente y se somete a una regulación adecuada, puede ser una herramienta efectiva para obtener pruebas y llevar a cabo investigaciones exitosas. Sin embargo, es importante que se establezcan límites y protocolos claros para evitar posibles abusos y proteger los derechos individuales.

a) Aspectos delimitadores del agente provocador y el delito provocado

Es fundamental que se establezca una definición precisa de la diferencia entre el agente encubierto y el agente provocador. Para ello, es importante comprender el delito provocado y delimitar el concepto de agente provocador, tanto desde la perspectiva de la doctrina penal como de la jurisprudencia de la Corte Constitucional del Ecuador.

Para comprender de manera integral el concepto de la figura del agente provocador es necesario correlacionar con la definición de lo que supone un delito provocado. En este sentido se ha definido al agente provocador como:

> […] aquel que llega a realizarse en virtud de la inducción engañosa de una determinada persona, generalmente miembro de las fuerzas de seguridad que, deseando la detención de sospechosos, incita a perpetrar la infracción a quien no tenía previamente tal propósito, originando así el nacimiento de una voluntad criminal en supuesto concreto, delito que de no ser por tal provocación no se hubiere producido aunque de otro lado su compleja ejecución resulte prácticamente imposible por la prevista intervención "ab initio" de la fuerza policial (Zafra Espinosa de los Monteros, 2010, p.100).

En este sentido, de acuerdo con el artículo 483, numeral 3, del COIP, se establece que:

> […] No será permitido al agente encubierto, persona jurídica encubierta y agente encubierto virtual impulsar delitos que no sean de iniciativa de los investigados, salvo en el caso de compras controladas, para lo cual el fiscal tendrá la facultad de definir la proporcionalidad y cantidad de la sustancia o bien a adquirir. (2014, art. 483 numeral 3)

La prohibición de utilizar medios ilícitos o reprochables en las actividades de investigación se basa en la idea de que estas acciones van en contra de los parámetros constitucionales del Estado de Derecho y constituyen una restricción a la legalidad del ius puniendi, según lo establecido en el artículo 11, numeral 9 de la Constitución de la República del Ecuador. Esto se fundamenta en que el Estado no puede emplear la incitación para cometer un ilícito a personas que no tenían la intención de cometerla, lo que resulta en la creación de la voluntad ilícita inexistente en un inicio y debido a ello se produce la comisión de un delito que previamente no habría ocurrido de no ser por la provocación (Zafra Espinoza de los Monteros, 2010). Desde la óptica procesal penal, todo el material probatorio obtenido contrario a la Constitución sería nulo, lo cual resultaría ilógico si se considera que la finalidad del agente encubierto informático es de indicios para probar la materialidad del delito y la responsabilidad del sujeto investigado en el ciberespacio.

De acuerdo con Zafra Espinoza de los Monteros (2010), "el agente encubierto debería ser el sujeto activo del delito provocado. Pero en realidad, estos términos de delito provocado y agente provocador representan realidades distintas" (p.104). Según la Corte Constitucional del Ecuador, se entiende como agente provocador como aquel funcionario que:

> […] interviene para inducir o incitar a cometer el delito (para la provocar la realización del delito) y su actuación determina que una o varias personas incurran en un delito que no tenían propuesto realizarlo con anterioridad, o en caso no hubiesen dado inicio formal a su preparación; mientras que el agente encubierto se infiltra en una organización criminal para determinar su estructura, funcionamiento e identificar a sus integrantes, esto es, para demostrar o acreditar que una o varias personas tenían ya la predisposición de realizar actividades ilícitas, o que continúan practicando dichas actividades y cuyo descubrimiento se pretende. El conocimiento y la voluntad de dirigir el comportamiento hacia la realización del hecho delictivo surge en este caso en la persona del autor vinculado al crimen organizado y no en el agente encubierto. (Corte Constitucional del Ecuador, 2021, sentencia No. CC-13-14-IN/21)

De esta forma, tomando en cuenta la jurisprudencia de la Corte Constitucional del Ecuador, se considera legítima la actuación del agente encubierto, siempre y cuando los hechos delictivos estén en proceso de preparación y el agente proceda únicamente con la finalidad de revelar su estructura, funcionamiento, métodos y herramientas usadas para el cometimiento de delitos que ya hayan sido realizados previamente a la provocación. Con respecto al tema de las compras controladas, resulta preponderante que se respete el principio de proporcionalidad y que se no actúe en base a meros indicios para evitar instigar al sujeto investigado a cometer un delito que no tenía planeado.

En conclusión, el agente encubierto tiene prohibido instigar o fomentar la comisión de un acto ilegal. La iniciativa debe provenir siempre de los sospechosos, ya que el objetivo del agente encubierto es detectar actividades delictivas y recopilar pruebas para perseguirlas y juzgarlas, lo que, a su vez, permitirá desmantelar grupos de ciberdelincuencia organizada o cibercriminales que actúan de manera individual. De esa forma, la conducta típica del agente provocador se basa el uso de medios de engaño, simulando intenciones ficticias, como, por ejemplo, la intención de comprar o vender material de abuso sexual infantil. Por lo tanto, su objetivo es crear un ilícito que

previamente no existía, cuando la finalidad del agente encubierto informático es descubrir uno que ya ha sido cometido previamente. Solo de esa manera su actuación se encuentra amparada por lo límites impuestos por la Constitución de la República del Ecuador y el COIP para realizar sus funciones de investigación criminal, develamiento de las operaciones criminales en el ciberespacio y la recolección de información sobre el presunto delincuente.

b) Ámbito de actuación del agente encubierto informático

El agente encubierto informático actúa en dos ámbitos del ciberespacio: canales abiertos de comunicación o ciberpatrullajes, y fuentes cerradas de comunicación o información. Según el artículo 483.1 del Código Orgánico Integral Penal, la infiltración y penetración del agente informático está limitada a las fuentes cerradas de comunicación e información.

> […] deberán realizar patrullajes o acciones digitales en el ciberespacio, penetrándose e infiltrándose en plataformas informáticas como foros, grupos de comunicación o fuentes cerradas de información o comunicación […].

Los miembros del Sistema especializado integral de investigación, de medicina legal y ciencias forenses pueden realizar patrullajes cibernéticos utilizando técnicas de Open Source Intelligence (OSINT) para recopilar información pública que pueda ser utilizada en la investigación criminal. No obstante, la función del agente encubierto informático reside en infiltrarse en canales cerrados de comunicación, como foros o grupos de chat, para lo cual se requiere autorización judicial de la autoridad competente.

En este sentido, las llamadas fuentes de comunicación en canales cerrados "se caracteriza por la expresa voluntad del comunicante de excluir a terceros del proceso de comunicación" (Carou, 2021, p.850). Las características de un canal cerrado de comunicación refieren a que los interlocutores deben aceptar previamente a cada persona que se une a su grupo de contactos de confianza. De esta manera, el interlocutor restringe el acceso a ciertos contenidos seleccionados

por él mismo, limitando su difusión solo a un grupo específico de personas. Esto se debe a que el modus operandi de los cibercriminales se realiza desde el anonimato y de manera confidencial, por lo cual hacen uso de foros cerrados o encriptados, lo cual dificulta su identificación por los agentes de seguridad. Por lo tanto, es idóneo que el agente encubierto informático se infiltre en estos canales cerrados de comunicación para interactuar con los participantes y recolectar evidencia respetando los principios de necesidad y proporcionalidad.

Cuando las fuentes de comunicación son abiertas, no es necesario acudir a la figura del agente encubierto informático, ya que la Policía Nacional puede rastrear los contenidos públicos de la red sin necesidad de una autorización adicional. Pues dicha autorización legislativa ha de considerarse comprendida, dentro de las facultades atribuidas a la Policía Nacional del Ecuador, por el artículo 158 inciso tercero de la Constitución de la República del Ecuador, el artículo 61 numeral 3 del COESCOP y el artículo 483.1 del COIP. Al respecto, la sentencia No. 2064-14-EP/21 de la Corte Constitucional, en el punto 116, define al espacio público:

> […] En definitiva, este puede ser definido como un lugar abierto, pues es de uso común, en donde las personas se reúnen con la finalidad de interactuar de distintas maneras e intercambiar sus ideas u opiniones e integrarse, claro está, con la limitación prevista en el referido artículo 23. Ahora bien, dado que se ejercen varios derechos a la vez, y que son espacios abiertos al público en general, la intimidad personal puede ser regulada, limitada o restringida en este tipo de espacio, con mayor facilidad. En este sentido, la calle o la vía pública son claros ejemplos de un espacio público. (p.16)

El acceso a información pública no requiere autorización judicial y cualquier usuario puede obtenerla ya que son ellos mismos quienes la han introducido en la red. El registro de entrada queda registrado y el mismo usuario lo sabe (Carou, 2021). Los entornos digitales tienen el mismo nivel de protección que los entornos físicos y, por lo tanto, deben ser tratados de manera similar al determinar el marco de protección. En este sentido, al referirse a redes sociales, foros abiertos en Internet y redes peer to peer, es necesario distinguir si el espacio es cerrado o abierto para definir el marco de protección correspondiente a la intimidad del usuario en dicho espacio.

En consecuencia, los agentes de la Policía Nacional del Ecuador están habilitados legalmente para llevar a cabo labores de ciberpatrullaje en fuentes de comunicación abiertas, interactuando con otros individuos a través de nombres ficticios sin requerir de autorización judicial. Esta actividad se enmarca en sus funciones legales de vigilancia y prevención del delito. Es importante destacar que, en la actualidad, los usuarios de Internet que se comunican con otros mediante apodos o sobrenombres aceptan implícitamente que la persona con la que se comunican no necesariamente se corresponde con su verdadera identidad (Carou, 2021).

Por otro lado, según lo establecido en el artículo 483.1 del Código Orgánico Integral Penal, la infiltración en línea tiene como objetivo la investigación de "hechos delictivos cometidos o que puedan cometerse con el uso o en contra de las tecnologías de la información y comunicación, esto es ciberdelitos puros o replicas o cualquier otro tipo de delito" (COIP, 2014). En comparación con su similar físico, el agente encubierto virtual tiene un espectro de actuación mucho mayor, debido a que en el artículo en mención señala que podrán ser "cualquier otro tipo de delito", abriendo la posibilidad de aplicar en los delitos que se considere idónea esta figura de investigación, diferenciándose de su homologo físico debido a que no existe la necesidad de existencia de un grupo de delincuencia organizada.

En relación a este asunto, se considera importante tener en cuenta que en el artículo 483.1 del COIP se hace referencia explícita a los "ciberdelitos puros o réplicas" (COIP, 2014), lo cual plantea interrogantes desde una perspectiva técnica legislativa, ya que no se comprende completamente el concepto de "ciberdelitos réplicas". Es posible que se trate de una alusión a los delitos cometidos por seres humanos en sistemas informáticos en general. En este sentido, la investigación de la distribución de pornografía infantil a través de Internet mediante operaciones encubiertas virtuales no tiene necesariamente que estar relacionada con una organización criminal.

c) Principios rectores del agente encubierto informático

La utilización de técnicas especiales de investigación para la resolución de delitos puede conllevar a la restricción de ciertos derechos fundamentales del individuo investigado. Sin embargo, antes de proceder a dicha limitación, es necesario que un juez valore y justifique la necesidad y proporcionalidad de dichas medidas, a través de una autorización judicial dictada con estricta sujeción a los principios de idoneidad, especialidad, necesidad y proporcionalidad.

Es relevante considerar que los principios mencionados previamente constituyen requisitos acumulativos, los cuales son guiados por múltiples interpretaciones de la Corte Constitucional del Ecuador. De este modo, es imprescindible satisfacer todos estos principios de forma simultánea, dado que, si se incumple cualquiera de ellos, se considerará que la medida tomada es nula. En lo que sigue, se presentarán las definiciones de cada uno de los principios mencionados.

Especialidad: En sentido amplio, este principio tiene su fundamento en la autorización judicial para la realización de diligencias de investigación tecnológica basado en la exigencia de una motivación previa basada en indicios de actividad criminal. Por lo tanto, no se permiten las diligencias tecnológicas preventivas, ya que esto podría llevar a un estado policial en el que todos se sientan vigilados. En consecuencia, la autorización para las diligencias de investigación tecnológica debe estar siempre relacionada con la investigación de un delito concreto, al menos en el plano indiciario (Bueno de Mata, 2019).

Por lo tanto, el principio de especialidad, en el marco de aplicación de las operaciones encubiertas informáticas refiere a la limitación del objeto de la investigación a los hechos que motivaron a la autorización judicial. Lo que significa que cualquier diligencia investigativa solo puede ser utilizada para la investigación del delito para lo cual fue autorizada por el Juez de Garantías Penales y no para otros fines. Lo que se traduce, en que la investigación se encuentre

limitada a los hechos en investigación, sin poder extenderse a otros hechos o delitos que no fueron incluidos.

Idoneidad: Este principio refiere a que las técnicas especiales de investigación que se utilicen deben ser las apropiadas para alcanzar el objetivo perseguido, es decir, deben ser efectivas y eficaces para la investigación del delito. Esto significa que no se pueden utilizar técnicas o medidas que resulten excesivas, innecesarias o desproporcionadas en relación con el delito investigado, ya que esto podría vulnerar los derechos fundamentales del investigado.

En este sentido, este principio ha sido desarrollado por la Corte Constitucional del Ecuador, en la Sentencia No. 13-14-IN/21, indicando que:

> […] En cuanto a la idoneidad, la Corte Constitucional ha sostenido que implica que la medida tomada sea adecuada para cumplir el fin constitucional, es decir, que sea conducente a la finalidad constitucionalmente válida. Al respecto, de lo mencionado anteriormente se observa que la Constitución de la República contempla el garantizar una cultura de paz, seguridad y prevención de todo tipo de violencia, así como prevenir el cometimiento de delitos como un fin válido; en este sentido, determinar al agente encubierto como una técnica de investigación especial y excepcional empleada para combatir el crimen organizado y brindar información desde el interior de estos grupos es una medida idónea para cumplir con tal fin. (p.32)

El artículo 483.1 del Código Orgánico Integral Penal (COIP) establece la finalidad del agente encubierto informático como la posibilidad de "descubrir, investigar o esclarecer hechos delictivos cometidos o que puedan cometerse con el uso o en contra de las tecnologías de la información y comunicación, esto es ciberdelitos puros o réplicas o cualquier otro tipo de delito" (COIP, 2023, art. 483 numeral 1). Por lo tanto, la figura del agente encubierto informático puede permitir al fiscal probar de manera razonable las circunstancias en que se ha cometido el delito y las personas responsables del mismo.

Necesidad: El empleo de agentes encubiertos informáticos por parte del Estado debe restringirse a lo que sea claramente necesario para lograr un objetivo legítimo. La utilización de operaciones

encubiertas en línea solo debería efectuarse únicamente cuando es estrictamente necesario y ya se haya agotado otras medidas, y que esta sea el que genere menor agravio a los derechos fundamentales. La responsabilidad de establecer esta justificación para otorgar de dicho autorización recae el Juez de Garantías Penales quien analizará la necesidad de esta figura, una vez que ha sido solicitada por la Fiscalía General del Estado.

Respecto a este principio la Corte Constitucional del Ecuador ha señalado que este:

> […] se presenta cuando dentro de las posibilidades válidas, la opción contenida en la norma es la de menor gravamen. Sobre esto, y como se indicó anteriormente, el crimen organizado se encuentra en constante evolución, las técnicas tradicionales empleadas para su investigación son insuficientes, debido a que estas organizaciones no cuentan solamente con recursos humanos, sino económicos y tecnológicos, que en algunas ocasiones superan a los recursos propios de los Estados; es en este sentido, que se vuelve necesario contar con técnicas especiales de investigación como son las operaciones encubiertas, las cuales se encuentran respaldadas, tanto en el orden internacional, como interno. (Corte Constitucional del Ecuador, 2021, sentencia No. CCE-13-14-IN/21)

En este sentido, el Tribunal Europeo de Derechos Humanos ha establecido el concepto del principio de necesidad. En la decisión dentro del caso: *Leander vs Suecia* reconoció que "el concepto de necesidad implica que la injerencia responda a una necesidad social acuciante y, en particular, que sea proporcionada con el fin legítimo que persigue" (TEDH, No. 9248/81, 1987).

Así mismo, en cuanto al concepto de *fin legítimo*, la Corte Constitucional del Ecuador ha señalado que:

> […] si una restricción o limitación tiene como "horizonte el cumplimiento de un objetivo" previsto en la Constitución o la promoción de derechos, es decir, que los fines para los cuales se establece la restricción deben ser legítimos en el sentido que "obedezcan a razones de interés general y no se aparten del propósito para el cual han sido establecidas" a luz del resto de disposiciones de carácter constitucional. (Corte Constitucional del Ecuador, 2021, sentencia No. 77-16-IN/21)

Por lo tanto, cuando se evalúa el principio de necesidad de una medida de investigación para abordar una necesidad urgente como la seguridad humana, es esencial analizar tanto su relevancia como su adecuación en relación con el fin legítimo.

Proporcionalidad: Por último, y como principio fundamental para la adopción de técnicas especiales de investigación, específicamente del agente encubierto informático. Aunque de manera sistemática con los otros principios, este es el de mayor relevancia pues este se encuentra correlacionado con los otros.

El análisis de este principio comienza con la comprensión de que los derechos establecidos en la Constitución de la República del Ecuador, específicamente en el artículo 66 numerales 19, 20, 21, y el artículo 77 numeral 7, literal c, no son derechos absolutos y, por lo tanto, pueden ser objeto de limitaciones. Sin embargo, dichas limitaciones deben ser proporcionales al objetivo de la investigación y no deben ser excesivas. Esto significa que, en algunos casos, estos derechos pueden ser limitados en favor de otros derechos constitucionalmente protegidos, como la seguridad ciudadana, la prevención del delito y la cultura de la paz. De esa manera, la noción de proporcionalidad, tal como se encuentra definida en el artículo 3 numeral 2 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, implica que se procure establecer un adecuado equilibrio entre, por un lado, la protección que se otorga a los derechos constitucionales y, por otro, las restricciones que se imponen sobre los mismos (LOGJCC, 2009).

En esta línea, el principio de proporcionalidad se relaciona con la necesidad de que el uso de agentes encubiertos en línea tenga más beneficios para la investigación que restricciones o costos a los derechos limitados. Para ello, se debe considerar el principio de mínima intervención penal y ponderar si, dadas las circunstancias del caso, la infiltración policial debe prevalecer sobre la restricción de esos derechos. Además, se deben tener en cuenta la naturaleza del delito investigado, las precauciones respecto al uso de la información obtenida, los supuestos en los que la información no relevante debe ser eliminada directamente por la Fiscalía General del Estado y el límite temporal necesario para limitar este derecho de manera razonable (Corte Constitucional del Ecuador, 2021,

CCE-77-16-IN/22). Por ello, en el ámbito digital, es importante que las restricciones a los derechos a la privacidad y a la protección de datos personales vayan de la mano con medidas de protección adecuadas para minimizar las posibles desventajas y riesgos asociados.

2.2. Derecho comparado: El agente encubierto informático en la legislación española

La inclusión de la figura del agente encubierto informático en el derecho procesal penal español se llevó a cabo a través de la modificación de la Ley de Enjuiciamiento Criminal (LECrim) del 14 de septiembre de 1882 mediante la Ley Orgánica 13/2015, de 5 de octubre. Esta figura está regulada en el apartado 6 del artículo 282 bis de la LECrim y se presenta como una técnica de investigación utilizada por la Policía Judicial que se encuentra entre la infiltración policial física y la intervención de las comunicaciones telemáticas. El objetivo de esta técnica es fortalecer las garantías procesales y regular las medidas de investigación tecnológica en el marco de la investigación criminal (Carou, 2021).

Según Federico Bueno de Mata (2019), la introducción de esta figura en España se relaciona con la lucha contra las bandas de pedófilos organizados en Internet que operan bajo organizaciones criminales. Debido a esta situación, la ley establece una distinción entre esta figura y otras medidas destinadas a combatir delitos cometidos por particulares, como las relacionadas con la captación y grabación de comunicaciones orales mediante dispositivos electrónicos. De igual manera, el uso de los agentes encubiertos informáticos se centra en la lucha contra el terrorismo, sobre todo la propaganda realizada en la darknet por parte de organizaciones Yihadistas.

Para efectos del análisis normativo, se ha tomado en cuenta un extracto del artículo en cuestión:

> 1. A los fines previstos en el artículo anterior y cuando se trate de investigaciones que afecten a actividades propias de la delincuencia organizada, el Juez de Instrucción competente o el Ministerio Fiscal dando cuenta inmediata al Juez, podrán autorizar a funcionarios de la Policía Judicial, mediante resolución fundada y teniendo en cuenta su

necesidad a los fines de la investigación, a actuar bajo identidad supuesta y a adquirir y transportar los objetos, efectos e instrumentos del delito y diferir la incautación de los mismos. La identidad supuesta será otorgada por el Ministerio del Interior por el plazo de seis meses prorrogables por períodos de igual duración, quedando legítimamente habilitados para actuar en todo lo relacionado con la investigación concreta y a participar en el tráfico jurídico y social bajo tal identidad.

La resolución por la que se acuerde deberá consignar el nombre verdadero del agente y la identidad supuesta con la que actuará en el caso concreto. La resolución será reservada y deberá conservarse fuera de las actuaciones con la debida seguridad.

La información que vaya obteniendo el agente encubierto deberá ser puesta a la mayor brevedad posible en conocimiento de quien autorizó la investigación. Asimismo, dicha información deberá aportarse al proceso en su integridad y se valorará en conciencia por el órgano judicial competente.

2. Los funcionarios de la Policía Judicial que hubieran actuado en una investigación con identidad falsa de conformidad a lo previsto en el apartado 1, podrán mantener dicha identidad cuando testifiquen en el proceso que pudiera derivarse de los hechos en que hubieran intervenido y siempre que así se acuerde mediante resolución judicial motivada, siéndole también de aplicación lo previsto en la Ley Orgánica 19/1994, de 23 de diciembre. Ningún funcionario de la Policía Judicial podrá ser obligado a actuar como agente encubierto.

3. Cuando las actuaciones de investigación puedan afectar a los derechos fundamentales, el agente encubierto deberá solicitar del órgano judicial competente las autorizaciones que, al respecto, establezca la Constitución y la Ley, así como cumplir las demás previsiones legales aplicables.

4. A los efectos señalados en el apartado 1 de este artículo, se considerará como delincuencia organizada la asociación de tres o más personas para realizar, de forma permanente o reiterada, conductas que tengan como fin cometer alguno o algunos de los delitos siguientes:

a) Delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos, previstos en el artículo 156 bis del Código Penal.

b) Delito de secuestro de personas previsto en los artículos 164 a 166 del Código Penal.

c) Delito de trata de seres humanos previsto en el artículo 177 bis del Código Penal.

d) Delitos relativos a la prostitución previstos en los artículos 187 a 189 del Código Penal.

e) Delitos contra el patrimonio y contra el orden socioeconómico previstos en los artículos 237, 243, 244, 248 y 301 del Código Penal.

f) Delitos relativos a la propiedad intelectual e industrial previstos en los artículos 270 a 277 del Código Penal.

g) Delitos contra los derechos de los trabajadores previstos en los artículos 312 y 313 del Código Penal.

h) Delitos contra los derechos de los ciudadanos extranjeros previstos en el artículo 318 bis del Código Penal.

i) Delitos de tráfico de especies de flora o fauna amenazada previstos en los artículos 332 y 334 del Código Penal.

j) Delito de tráfico de material nuclear y radiactivo previsto en el artículo 345 del Código Penal.

k) Delitos contra la salud pública previstos en los artículos 368 a 373 del Código Penal.

l) Delitos de falsificación de moneda, previsto en el artículo 386 del Código Penal, y de falsificación de tarjetas de crédito o débito o cheques de viaje, previsto en el artículo 399 bis del Código Penal.

m) Delito de tráfico y depósito de armas, municiones o explosivos previsto en los artículos 566 a 568 del Código Penal.

> n) Delitos de terrorismo previstos en los artículos 572 a 578 del Código Penal.
> o) Delitos contra el patrimonio histórico previstos en el artículo 2.1.e de la Ley Orgánica 12/1995, de 12 de diciembre, de represión del contrabando.
> 5. El agente encubierto estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de esta y no constituyan una provocación al delito. Para poder proceder penalmente contra el mismo por las actuaciones realizadas a los fines de la investigación, el Juez competente para conocer la causa deberá, tan pronto tenga conocimiento de la actuación de algún agente encubierto en la misma, requerir informe relativo a tal circunstancia de quien hubiere autorizado la identidad supuesta, en atención al cual resolverá lo que a su criterio proceda.
> 6. El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a.
> El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos.
> 7. En el curso de una investigación llevada a cabo mediante agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio.

Al igual que en la normativa ecuatoriana, no existe una definición expresa sobre el agente encubierto informático, únicamente haciendo referencia a temas como el ámbito de actuación, el modus operandi y el intercambio de archivos ilícitos, lo cual se encuentra expresamente recogido en el artículo 282 numeral 6 de la Ley de Enjuiciamiento Criminal: […] el agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos (LECrim, 2015). Esta opción es fundamental para alcanzar la finalidad perseguida por esta figura legal. Pues en relación a esta figura, es relevante considerar la importancia de la opción de infiltrarse en redes de distribución de pornografía infantil. En estos casos, es común que para formar parte de estos foros cerrados sea necesario enviar o intercambiar contenido de este tipo para ganar la confianza necesaria (Temperini, 2019). De esta forma, se genera el ambiente adecuado para llevar a cabo tareas de recolección de información por parte del agente encubierto informático.

En cuanto al ámbito de aplicación de esta figura, el agente encubierto informático difiere del agente encubierto convencional respecto a su ámbito de actuación. A diferencia del primer caso, el segundo está limitado a un conjunto cerrado de delitos que se encuentran en el artículo 282 bis 4 de la Ley de Enjuiciamiento Criminal (LECrim), mientras que la figura del agente encubierto informático, según el apartado 6 del mismo precepto, incluye una lista abierta de delitos que pueden ser objeto de investigación a través de esta técnica, sin que sea necesaria la acreditación de la delincuencia organizada en todos los casos (Carou, 2021). En el numeral sexto del artículo 282 bis, de manera expresa señala que el ámbito de actuación del agente encubierto informático se reduce a los "canales cerrados de comunicación", para lo que previamente se requerirá de la autorización del jueza para su infiltración.

Sin embargo, para el autor Bueno de Mata (2019), "si existe una figura con una regulación parca e incompleta, tanto en la LECrim tras la reforma del 2015 como en las Circulares del 2019, es la del agente encubierto en internet" (p.110). Pues el tema no fue abordado como debería, dejando algunas interrogantes como: ¿quién puede ser agente encubierto informático?, ¿qué características debe tener?, ¿a qué se refiere con archivo ilícito?, ¿cuál debe ser su modus operandi?, entre otras. En conclusión, se sostiene que hay diversas cuestiones que todavía deben resolverse a nivel jurisprudencial en relación a la figura del agente encubierto informático, independientemente de las menciones a intercambios ilegales de archivos. Es necesario definir con precisión el alcance de esta figura mediante una serie de categorías delictivas en las que pueda intervenir, lo que permitiría una regulación combinada entre los delitos específicos para el agente encubierto en el terreno físico y la cláusula abierta que se aplica a cualquier delito informático de acuerdo con la normativa actual para el bloque de diligencias de investigación (Bueno de Mata, 2019).

Capítulo III. Efectos en los Derechos Humanos en la era digital: derecho a la intimidad personal y familiar y protección a los datos personales: autodeterminación informativa

3.1. Derecho a la intimidad personal y familiar

La actuación del agente encubierto informático como diligencia de investigación criminal puede limitar ciertos derechos fundamentales de las personas investigadas. Por esta razón, es necesario que a esta se le otorgue la debida autorización judicial para llevar a cabo la actividad de infiltración, la misma que es justificada por el mismo hecho de que la infiltración policial limitará el alcance de ciertos derechos en el ámbito digital como la intimidad personal y familiar y la protección a los datos personales.

En este sentido, la actuación engañosa de los agente encubiertos informáticos, mediante el uso de una identidad falsa o *nickname* en el ámbito digital, les permite obtener la aprobación y confianza de los sujetos investigados o integrantes de la organización criminal. Esto con la finalidad de establecer relaciones personales que permitan su labor de infiltración, podría suceder que estas trasciendan a un plano informal donde se conozca información intima de la persona investigada como la preferencia sexual, hobbies, entre otros. El uso de técnicas de engaño por parte de los agentes encubiertos informáticos les facilita obtener acceso a aspectos íntimos de las personas investigadas (Carou, 2021).

Por lo tanto, para medir el grado de afectación a los derechos fundamentales del investigado dependerá del tipo de relación que mantiene el agente encubierto con el sujeto investigado o los integrantes de la organización criminal. Además, es importante analizar el rol que desempeñara el agente encubierto con el sujeto investigado (Zafra, 2014).

El reconocimiento del derecho a la intimidad, proclamado en el artículo 66 numeral 20 de la Constitución del Ecuador, implica "[…] la existencia y goce de una órbita reservada para cada persona, exenta del poder de intervención del Estado o de las intromisiones arbitrarias de la sociedad, que le permita a dicho individuo el pleno desarrollo de su vida personal" (Corte Constitucional del Ecuador, 2021, sentencia No. 2064-14-EP/21). Es decir, la intimidad se refiere a la capacidad de mantener en privado aspectos personales y familiares, de tal manera que no sean conocidos por terceros, incluyendo el Estado y otras entidades, o bien, si son conocidos, que no sean divulgados.

El derecho a la intimidad, al igual que cualquier otro derecho fundamental, implica una obligación por parte de los poderes públicos de respetar y garantizar la vida privada de las personas. Este derecho busca proteger la libertad individual y, por ende, se considera un derecho de defensa (Zafra Espinoza de Los Monteros, 2014). Sin embargo, el derecho a la intimidad no es absoluto y puede estar limitado en casos en lo que exista una finalidad legitima, como la investigación criminal o la seguridad nacional. En este sentido la Corte Interamericana de Derechos Humanos en el caso *Santander Tristán Donoso vs Panamá* se ha pronunciado al respecto al señalar que:

> El derecho a la vida privada no es un derecho absoluto y, por lo tanto, puede ser restringido por los Estados siempre que las injerencias no sean abusivas o arbitrarias; por ello, las mismas deben estar previstas en ley, perseguir un fin legítimo y cumplir con los requisitos de idoneidad, necesidad y proporcionalidad, es decir, deben ser necesarias en una sociedad democrática. (Tristán Donoso vs. Panamá, Serie C No. 193, 2009, párr. 56)

Por tanto, en situaciones en las que se presenten dos derechos fundamentales constitucionalmente protegidos, incluyendo el derecho a la intimidad, es necesario que el Juez de Garantías Penales examine diversos aspectos para determinar la justificación de una posible interferencia en la intimidad. Algunos de estos aspectos son: si dicha interferencia se encuentra

"prevista en la ley, si persigue una finalidad legítima y si resulta idónea, necesaria y proporcional en relación a los objetivos que se pretenden alcanzar" (Corte Constitucional del Ecuador, 2021, sentencia No. 2064-14-EP/21).

Siendo así que, los elementos que integran este derecho son: "derecho subjetivo y derecho de defensa; garantía institucional de pluralismo y democracia; derecho positivo; garantía de libertad; fundamento del orden social" (Zafra, 2010, p.172). Esta libertad, por supuesto, implica una doble responsabilidad del Estado, tanto en sus obligaciones activas como pasivas.

En cuanto a la esfera u obligación positiva del Estado, la Corte Constitucional del Ecuador ha señalado que:

> […] hace referencia a la obligación que éste tiene de implementar todas las medidas y ejercer todas las actuaciones posibles y necesarias para asegurar que el derecho a la intimidad se respete por parte de los funcionarios que representan al Estado. (Sentencia No. 2064-14-EP/21, 2021)

Por lo tanto, se requiere la implementación de salvaguardas para utilizar la figura del agente encubierto informático como técnica especial de investigación. Específicamente, es necesario una resolución judicial debidamente motivada que haga alusión y énfasis en los principios de proporcionalidad, idoneidad, excepcionalidad y necesidad de la medida para evitar arbitrariedades por parte de los funcionarios públicos e injerencias innecesarias al derecho a la intimidad.

En el mismo sentido, la esfera u obligación negativa del Estado en relación al derecho a la intimidad, según la Corte Constitucional del Ecuador consiste en:

> […] que el mismo debe abstenerse de realizar cualquier tipo de actividad o adoptar cualquier medida que pueda menoscabar este derecho, claro está, siempre que no se satisfagan los requisitos detallados en el párrafo 109 de la presente sentencia.[2] (Sentencia No. 2064-14-EP/21, 2021)

[2] Se puede restringir el derecho a la intimidad, siempre que la restricción no sea abusiva ni arbitraria; es decir, las limitaciones impuestas deben estar previstas en la ley, perseguir un fin legítimo y, por último, deben cumplir con

De igual manera, el 31 de octubre de 2016, la Asamblea General de las Naciones Unidas aprobó la resolución No. A/C.3/71/L.39 en la que señala que:

> […] los derechos de las personas, incluido el derecho a la privacidad, también deben estar protegidos en Internet y que, aunque la vigilancia no es en sí misma una violación de los derechos humanos, cualquier limitación del derecho a la privacidad debe respetar los principios generales de legalidad, necesidad y proporcionalidad. (p.3)

Además, que:

> […] la vigilancia de las comunicaciones digitales debe ser compatible con las obligaciones internacionales en materia de derechos humanos y debe llevarse a cabo sobre la base de un marco jurídico que sea de acceso público, claro, preciso, amplio y no discriminatorio, y que ninguna injerencia en el derecho a la privacidad debe ser arbitraria o ilegal, teniendo en cuenta lo que sea razonable para la persecución de objetivos legítimos. (p.4)

En consecuencia, para aplicar la figura del agente encubierto informático se requiere una finalidad legitima, como la prevención de infracciones y delitos, como parte del deber de servicio público de seguridad, al igual que el deber subjetivo del Estado de "garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral y a vivir en una sociedad democrática y libre de corrupción" (CRE, 2008, art. 3 numeral 8). Estos derechos pueden encontrarse en colisión con el derecho a la intimidad de la persona investigada, por lo que será el Juez de Garantías Penales quien deberá analizar la proporcionalidad de la medida en base a cada uno de los principios para establecer si se cumple con la finalidad legítima.

Por otro lado, se debe considerar que el derecho a la intimidad se incluye dentro de los derechos de la personalidad, que también incluyen a la dignidad y autodeterminación informativa (Muñoz, 2015). Este derecho se encuentra correlacionado con la libertad de las personas. En este sentido, las dimensiones en las cuales se puede proyectar el derecho a la intimidad pueden ser "(i) como secreto que impide la divulgación ilegítima de hechos o documentos privados, o (ii) como libertad,

---

los requisitos de idoneidad, necesidad y proporcionalidad. (Corte Constitucional del Ecuador, 2021, Sentencia No. 2064-14-EP/21, 2021)

que se realiza en el derecho de toda persona a tomas las decisiones que conciernen a la esfera de su vida privada (Corte Constitucional de Colombia, 1992, sentencia No. T-222).

En este contexto, es necesario hacer una distinción en los conceptos de intimidad y privacidad, mismos que representan dos aspectos diferentes del derecho a la intimidad. El término privacidad hace referencia al respeto por la vida privada, la divulgación de esta y el control del acceso a ella (Zafra, 2015). Este concepto fue desarrollado en el derecho anglosajón como "the right to be let alone", “lo que significa el derecho de toda persona a no ser molestada en su soledad, o, en otras palabras, el derecho a estar solo sin interferencias y protegido contra la observación intrusiva” (Sorokin, 2022, p.17).

Mientras que, la intimidad “hace referencia a las relaciones de intimidad entablada con otras personas” (Zafra, 2014, p.173), la intimidad “constituye la existencia, goce y disposición de una esfera reservada para el individuo” (Corte Constitucional del Ecuador, 2021, Sentencia No. 77-16-IN/22).

De manera más clara, para Cobos (2013) la diferencia del derecho a la intimidad y del derecho a la privacidad consiste en que: “el primero está relacionado con el comportamiento social de la persona e involucra aspectos personales o familiares e implica sentimientos, pensamientos, sexualidad y sus secretos más reservados; el segundo requiere de la proyección pública de su titular para hacerse efectivo” (p. 45).

Ahora bien, la Corte Constitucional de Ecuador reconoce que el derecho a la intimidad puede manifestarse en distintos contextos y, por ende, debe ser protegida de manera diferenciada. Esto implica que la protección del derecho a la intimidad puede variar según el espacio en el que se encuentre una persona y el contexto en el que se manifieste o actúe. Estos espacios pueden ser

públicos, privados o híbridos (semi-privados o semi-públicos). (CCE, sentencia No. 2064-14-EP/21, 2021)

En este contexto, el espacio público puede ser definido como:

> […] un lugar abierto, pues es de uso común, en donde las personas se reúnen con la finalidad de interactuar de distintas maneras e intercambiar sus ideas u opiniones e integrarse, claro está, con la limitación prevista en el referido artículo 23. Ahora bien, dado que se ejercen varios derechos a la vez, y que son espacios abiertos al público en general, la intimidad personal puede ser regulada, limitada o restringida en este tipo de espacio, con mayor facilidad. En este sentido, la calle o la vía pública son claros ejemplos de un espacio público. (CCE, sentencia No. 2064-14-EP/21, 2021)

Por lo tanto, en el caso de la esfera pública, "se incardinan aquellos datos íntimos o no, que el particular desee exteriorizar al público en general" (Zafra, 2014, p.174). En este caso, la intimidad personal puede ser limitada con mayor facilidad, pues se puede permitir un grado de inferencia por parte del Estado. En el caso de la tecnología o redes sociales, al tratarse de un espacio virtual, habrá que determinar si "aquel es cerrado o abierto y, por ende, fijar el marco de protección del que goza la intimidad del individuo que se desenvuelve en dicho espacio" (Corte Constitucional del Ecuador, 2021, sentencia No. 2064-14-EP/21).

En el caso del espacio privado, este es:

> […] aquel lugar cerrado al público en general, limitando su acceso a personas específicas y concretas, donde lógicamente quien toma esa decisión, por lo general, es el propietario, residente o habitante del lugar. Así, en este tipo de espacio la persona ejerce sus derechos con mayor libertad, principalmente la intimidad, con lo cual, la restricción al derecho referido debe ser excepcional. Por consiguiente, un ejemplo de espacio privado es el domicilio de una persona o también "[...] todos aquellos espacios cerrados, en donde las personas desarrollan de manera más inmediata su intimidad y su personalidad mediante el ejercicio de su libertad". Cabe destacar que los espacios virtuales gozan de la misma protección que los físicos y, además, deben ser analizados con la misma lógica a la hora de determinar su marco de protección. (CCE, sentencia No. 2064-14-EP/21, 2021)

La Corte Constitucional del Ecuador establece que la limitación al derecho a la intimidad debe ser de carácter excepcional, cumplir con los principios enunciados previamente, y perseguir un fin

legítimo para su restricción. Pues, en el marco de la infiltración del agente encubierto informático este provocaría una injerencia en el derecho a la intimidad, debido a que en el ámbito privado el sujeto investigado podría indicar la faceta de su personalidad más íntima, pudiendo conocer sus sentimientos, los pensamientos y sus relaciones personales y familiares, es decir su vida personal.

Dentro del contexto de la infiltración policial, la privacidad puede ser comprometida desde el inicio de la operación encubierta, incluso de manera inevitable. La restricción de la intimidad dependerá de la relación que establezca el agente encubierto con el sujeto investigado (Zafra, 2014). Si la investigación se realiza de forma pasiva, sin establecer ninguna relación personal, en un inicio no se estaría violando el derecho a la intimidad. Por lo tanto, es responsabilidad del Juez de Garantías Penales garantizar que la infiltración policial no afecte de manera desproporcionada el derecho a la intimidad personal, evitando así arbitrariedades por parte de funcionarios públicos o injerencias innecesarias.

3.2. Derecho a la protección de los datos personales en el marco de la investigación criminal: autodeterminación informativa.

El Tribunal Constitucional Federal de Alemania utilizó por primera vez el concepto de derecho a la autodeterminación informativa en su sentencia sobre la Ley del Censo del 15 de diciembre de 1983, con la que se faculto a las personas a decidir y consentir de forma informada y libre el uso de sus datos personales por terceros, es decir que tiene su fundamento en el libre desarrollo de la personalidad (Corte Constitucional del Ecuador, sentencia No. 001-14-PJO-CC, 2014). Este derecho es prácticamente nuevo pues nace por el uso masivo de los sistemas informáticos, ampliando de esta manera el contenido del derecho a la intimidad, pues la concepción de este derecho se ve superado por las tecnologías de la información y sus diversos usos para procesar, distribuir, conservar o difundir datos personales. Además, el derecho a la autodeterminación

informativa se encuentra de cierta manera anclado al derecho a la honra y el buen nombre, sin embargo, es importante resaltar que este derecho es autónomo de estos dos.

Es así, que este derecho alcanza un rango constitucional, el mismo que se reconocido en el artículo 66 numeral 9 de la Constitución de la República del Ecuador:

> El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (CRE, 2008, art. 66 numeral 9)

La jurisprudencia de la Corte Constitucional del Ecuador ha establecido con precisión que el derecho a la autodeterminación informativa es la base fundamental del derecho a la protección de datos personales. Igualmente, en la actualidad, ambos derechos han sido como sinónimos para referirse a un mismo concepto (Corte Constitucional del Ecuador, sentencia No. 2064-14-EP/21, 2014).

Por lo tanto, el derecho a la autodeterminación informativa supone en palabras de la Corte Constitucional del Ecuador:

> […] parte del derecho a la protección de datos personales, implica la necesidad de garantizar la protección de la esfera íntima de las personas, así como la posibilidad de ejercer control sobre los datos personales del sujeto, aunque no se encuentren en su poder. (Corte Constitucional del Ecuador, sentencia No. 001-14-PJO-CC, 2014)

En materia de desarrollo jurisprudencia constitucional en relación a este derecho es escasa en el ámbito ecuatoriano, sin embargo, en la legislación colombiana se define a este derecho como:

> […] la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales. (Corte Constitucional de Colombia, 1995, Sentencia No. SU-082/95)

Por lo tanto, resulta obvio, que, en el marco de las infiltraciones policiales, el derecho a la autodeterminación informativa pueda verse afectado, ya que durante una operación encubierta se pueden recopilar y tratar datos personales de los sujetos investigados sin su consentimiento previo.

Estos datos pueden ser utilizados para recopilar información sobre la vida privada de la persona, sus relaciones personales y su entorno, lo que puede resultar en una limitación de su derecho a la privacidad y a la protección de datos personales (Carou, 2021). Además, al no conocer información básica como su interlocutor, debido a que el agente encubierto online opera bajo un seudónimo limita la posibilidad de ejercer control de sus datos personales.

Sin embargo, es importante destacar que, si bien la realización de infiltraciones policiales puede estar justificada en determinadas circunstancias, como en casos de investigación de delitos graves, es necesario que se realicen bajo los principios de excepcionalidad, proporcionalidad y necesidad, y siempre dentro del marco de los derechos fundamentales de las personas.

IV. Conclusiones

El uso de tecnologías de información y comunicación en el siglo XXI ha impulsado el crecimiento económico, político y social, abarcando campos antes inimaginables como el teletrabajo y los servicios médicos en línea. Sin embargo, desafortunadamente, individuos inescrupulosos o grupos del crimen organizado están aprovechando de forma ilícita el ciberespacio, trasladando actividades previamente realizadas en el mundo físico al ámbito digital, como el tráfico de personas, sustancias y estafas. Estos actores criminales aprovechan el anonimato que ofrece el ciberespacio generando una sensación de seguridad para sus actividades delictivas y de impunidad para quienes son víctimas de ellos.

Por lo tanto, debido a la falta de herramientas de investigación penal en la actualidad, los legisladores ecuatorianos han regulado de forma incompleta la investigación criminal en el ciberespacio. Siendo así que, mediante la Ley Orgánica Reformatoria a varios cuerpos legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral, publicada en el

Suplemento del Registro Oficial No. 279 el 29 de marzo de 2023, se introduce reformas al Código Orgánico Integral Penal, específicamente en relación con la investigación de delitos cibernéticos. Una de las modificaciones más significativas es la inclusión de la figura del agente encubierto informático, que permite investigar delitos cibernéticos puros o replicas, en contraste con las prácticas previas que se limitaban al uso de agentes encubiertos en entornos físicos.

En este sentido, esta técnica especial de investigación tiende a ser restrictiva de derechos humanos, por lo tanto, se requiere de un análisis meticuloso por parte de los Jueces de Garantías Penales para su adopción. Quienes a través de una resolución de manera motivada con todos los presupuestos establecidos en la ley y en la jurisprudencia constitucional, con especial énfasis en los principios de proporcionalidad, necesidad, especialidad e idoneidad para evitar injerencias innecesarias y actuaciones arbitrarias por parte de funcionarios públicos. En sentido estricto, lo que se busca a través de una autorización por parte de un Juez de Garantías Penales es evitar por un lado el abuso de esta técnica especial de investigación, y además procurar que todos los elementos obtenidos durante la infiltración policial no sean contrarios a la Constitución de la República del Ecuador.

Además, que, para el correcto funcionamiento de esta figura de investigación, es importante que los miembros del Sistema Especializado Integral de Investigación, de Medicina Legal y Ciencias Forenses se encuentren capacitados y que cuenten con los recursos económicos y técnicos para realizar la infiltración policial en internet, pues su instancia en la red es durante un período prolongado de tiempo, debido a que los grupos cibercriminales, especialmente en aquellos foros de la red oscura donde la confianza es la base de las relaciones criminales es donde el agente encubierto informático quien mediante engaños pretenderá ser un colega. Por lo tanto, las unidades especializadas tanto de la Fiscalía General del Estado como del Sistema Especializado Integral de

Investigación, de Medicina Legal y Ciencias Forenses deberán recibir capacitaciones en el ámbito informático, técnico y jurídico.

Finalmente, el carácter transnacional de los ciberdelitos da a comprender que para utilizar esta figura es necesario fortalecer la cooperación internacional y así poder armonizar el régimen jurídico penal en el Ecuador en concordancia con el resto de los países. Considerando que en la actualidad el Estado Ecuatoriano aún no ha ratificado la Convención contra la Ciberdelincuencia de Budapest, siendo complicado acceder a la cooperación internacional en esta materia por lo que se deberá optar por otros mecanismos de intercambio de información a través de conductos mediante INTERPOL. Así este organismo servirá para intercambio de información en materia de investigación penal, especialmente en aquellos delitos que sean de carácter transfronterizo, como la trata de personas, el tráfico de estupefacientes, entre otras actividades que abarcan a grupos de delincuencia organizada.

V. Recomendaciones

A pesar de que la figura del agente encubierto informático ya fue integrada dentro del ordenamiento jurídico penal ecuatoriano aún falta desarrollo mayor, por lo que se alienta al legislador a un desarrollo integral y ajustado a la realidad ecuatoriana en relación a las técnicas de investigación penal en el siglo XXI. Pues aún caben muchas interrogantes en relación a la facultad de intercambiar, enviar de manera directa archivos, ficheros con contenido ilícito, ¿qué se entiende por archivos o ficheros con contenido ilícito?, puede ser una referencia al envió de ficheros que tengan programas maliciosos como medio de interceptación de datos, o también conocido en la legislación española como el registro remoto mediante troyanos, situación a la cual no se encuentra habilitado el agente encubierto informático, y que es de suma importancia en la investigación

penal. Por lo tanto, es necesario integrar de manera urgente el registro remoto para cumpla con el principio de legalidad.

Además, en los casos donde el agente encubierto informático tenga que intercambiar archivos ilícitos como material de abuso sexual de menores, ¿qué herramientas usaran para crear contenido que parezca creíble?, ¿cómo van a dar seguimiento a dicho contenido para que no sea difundido en la red?, para solventar este tema en España se ha optado por usar actores que tengan características o sean similares a menores de edad, o el uso de inteligencia artificial para recrear escenas; pues existen ocasiones donde la única manera de encontrar a ciberdelincuente que crean o difunden material pedófilo es a través de la infiltración policial en dichos foros cerrados. Y es en estos sitios donde únicamente admiten entre sus miembros a personas que comparten cierta cantidad de material sensible, cuestión que es solventada con la reforma de la actualidad pues habilita al agente encubierto informático al intercambio de archivos ilícitos. Para dar seguimiento a estos archivos es necesario de un trabajo multidisciplinario con peritos expertos en informática para que sean ellos quienes puedan recuperar dichos archivos.

Finalmente, si bien es cierto que el Ecuador se encuentra como miembro observado por parte de la Comunidad Europea para adherirse a la Convención sobre Ciberdelincuencia es necesario trabajar en la integración normativa para cumplir con los parámetros necesarios y contar con los mecanismos de cooperación internacional otorgados por dicha Convención, pues al ser una medida de carácter transfronterizo es relevante contar con el apoyo de otros Estados para la lucha efectiva contra la ciberdelincuencia y la recolección de material probatorio en otros lugares.

Referencias

Acurio, S. (2003). *Delitos informáticos: generalidades,* 12 (1), (pp. 2). Recuperado de *http://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/599*

Acosta, A. (18 de octubre de 2019). Dark web: en los callejones de la red. ***El Tiempo.*** Recuperado https://www.eltiempo.com/tecnosfera/dispositivos/deep-web-en-los-callejones-de-la-red-363246

Asamblea General de Naciones Unidas. (2020). *Cooperación internacional mediante técnicas especiales de investigación,* 1 (1), (pp. 2) Recuperado de CTOC_COP_WG.3_2020_3_S.pdf (unodc.org)

Asamblea General de las Naciones Unidas. (2013). *El derecho a la privacidad en la era digital*, 1 (1), (pp.3-4) Recuperado de https://digitallibrary.un.org/record/848969/files/A_C-3_71_L-39_Rev-1-ES.pdf?ln=es

Aguilar, A, Benites, E, Scotti, L., y Sorokin, P. (2022). La Privacidad como derecho humano contribuciones para la promoción de una nueva agenda bioética. *A modo de proemio,* 1 (1), (pp. 17). DOI: 10.22201/fpsi.20074778e.2022.1.21.77790

Alazab, M, Broadhurst, R, Chon, S., y Grabosky, P. (2014). *Organisations and Cybercrime: An Analysis of the Nature of Groups Engaged in Cybercrime*. Recuperado de https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2461983_code1830215.pdf?abstractid=2461983&mirid=1

Asamblea Nacional del Ecuador. Código Orgánico Integral Penal. [Codificación 18]. (10 de Febrero 2014). RO. Suplemento 20 de 16 marzo de 2022.

Asamblea Nacional del Ecuador. Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. [Ley 0 del 2009]. (22 de octubre de 2009). RO. Suplemento 52 de 22 de octubre de 2009.

Asamblea Nacional del Ecuador. Ley Orgánica Reformatoria a varios cuerpos legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral. [Codificación 1]. (29 de marzo de 2023). RO. Suplemento 279 de 29 de marzo de 2023.

Bueno de Mata, F. (2011). *El Agente Encubierto en Internet: Mentiras Virtuales para Alcanzar la Justicia,* 9 (3), (pp. 302). Recuperado de http://hdl.handle.net/2183/9179

Bueno de Mata, F. (2019). *Las diligencias de investigación penal en la cuarta revolución industrial*. Pamplona, España: Arazandi, S.A.U.

Beniger, J. (1989). *The Control Revolution: Technological and Economic Origins of the Information Society*. Londres, Inglaterra: Harvard University Press.

Cobos, P. (2013). Cuestiones Constitucionales. *El contenido del derecho de intimidad,* 1 (1), (pp. 46-47). DOI: 10.1016/S1405-9193(13)71290-3

Chabinsky, S. (23 de marzo 2010). Speeches. *The Cyber Threat: Who's Doing What to Whom?,* 1 (1), (pp. 1). Recuperado de https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom

COE. (2001). *Informe Explicativo del Convenio sobre Ciberdelincuencia*. Recuperado de https://rm.coe.int/16802fa403

Constitución de la República del Ecuador [Const.]. (2008). 8va Ed. Recuperado de https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

EUROPOL. (2020). *Internet Organised Crime Threat Assessment (IOCTA)*. Recuperado de https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

Ministerio de Relaciones Exteriores. Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos. [Codificación 1275]. (23 de Abril del 2002). RO. 153 de 25 noviembre de 2005.

Corte Nacional de Justicia, Sala de Casación Penal. (13 de mayo del 2011) Resolución No. 011-2013. [Dra. Lucy Blacio Pereira].

Corte Nacional de Justicia, Sala de Casación Penal. (11 de marzo de 2011) Resolución No. 1453-2012. [Dr. Merck Benavidez Benalcázar].

Corte Constitucional del Ecuador. (27 de enero de 2022) Sentencia No. 77-16/IN-22. [Dr. Enrique Herrería Bonnet].

Corte Constitucional del Ecuador. (27 de enero de 2021) Sentencia No. 2064-14/EP/21. [Dra. Carmen Corral Ponce].

Corte Constitucional del Ecuador. (08 de diciembre de 2021) Sentencia No. 13-14-IN/21. [Dra. Carmen Corral Ponce].

Corte Constitucional de Colombia. (1 de marzo de 1995) Sentencia No. SU-082/95. [Dr. Jorge Arango Mejía].

Corte Constitucional de Colombia. (10 de marzo de 1992) Sentencia No. T-222. [Dr. Ciro Angarita Barón].

Rosa Cortina, J. (2011). *Los delitos de pornografía infantil. Aspectos penales, procesales y criminológicos*. Valencia, España: TIRANT LO BLANCH.

Espinoza, Z. (2010). *El policía infiltrado: Los presupuestos jurídicos en el proceso penal español.* Valencia, España: TIRANT LO BLANCH

Fernández, D., Carou, S., y Sanz, E. (2021). *Tratado de Delincuencia Cibernética: Cibercriminalidad e investigación Policial. El agente encubierto informático.* Pamplona, España: Arazandi, S.A.U.

Fiscalía General del Estado. (2021). *Perfil Criminológico: Ciberdelitos.* Recuperado de https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

Galán, A. (2020). *Los ciberdelitos en el ordenamiento español.* Barcelona, España: UOC.

INTERPOL. (2021). *National Cybercrime Strategy: Guidebook.* Recuperado de https://www.interpol.int/content/download/16455/file/Cyber%20Strategy%20Guidebook.pdf

INTERPOL. (2017). *Global Cybercrime Strategy: Anonymity Networks.* Lyon, Francia: INTERPOL GENERAL SECRETARIAT.

ICMEC. (2018). *Material sobre abuso sexual infantil: legislación modelo y revisión global.* Recuperado de https://www.icmec.org/wp-content/uploads/2019/12/Material-Sobre-Abuso-Sexual-Infantil-Legislacion-Modelo-y-Revision-Global-9na-Ed.pdf

Lusthaus, J. (2018). *Industry of Anonymity: Inside the business of Cybercrime.* Londres, Inglaterra: Harvard University Press.

Montoya, M. (1998). *Informantes y técnicas de investigación encubiertas; análisis constitucional y procesal penal*. Buenos Aires: AD-HOC.

Mendoza, B. (2001). *El derecho penal en la sociedad del riesgo.* Madrid, España: Civitas Ediciones S.L.

Maras, M. (2016). *Cybercriminology*. Nueva York, Estados Unidos: Oxford University Press Inc.

McClean, D. (2007). *Transnational Organized Crime: A commentary on the UN Convention and its Protocols.* Nueva York, Estados Unidos: Oxford University Press Inc.

Muñoz, S. (2021). *Trabajo final: Plan de disertación completo*. (Trabajo de la materia de Proyecto Integrador IV). Pontificia Universidad Católica del Ecuador: Quito, Ecuador.

Oficina de Naciones Unidas contra la Droga y el Delito. (2022). *Compendio de ciberdelincuencia organizada.* Recuperado de https://www.unodc.org/documents/organized-crime/tools_and_publications/21-05345_S_eBook.pdf

Oficina de Naciones Unidas contra la Droga y el Delito. (2020). Modulo 1: Introducción a la Ciberdelincuencia. *La ciberdelincuencia en resumen,* 2 (1), (pp. 1). Recuperado de Cybercrime Module 1 Key Issues: Cybercrime in Brief (unodc.org)

Oficina de Naciones Unidas contra la Droga y el Delito. (2020). *Darknet Cybercrime Threats to Southeast Asia*. Recuperado de https://www.unodc.org/roseap/uploads/documents/Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf

Oficina de Naciones Unidas contra la Droga y el Delito. (2013). *Estudio exhaustivo sobre el delito cibernético.* Recuperado de https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf

Oficina de Naciones Unidas contra la Droga y el Delito. (2012). *Compendio de casos de delincuencia organizada.* Recuperado de https://www.unodc.org/documents/organized-crime/SpanishDigest_Final291012.pdf

Posada, R. (2017). *Los cibercrímenes: Un nuevo paradigma de criminalidad.: Un estudio del título VII bis del Código Penal colombiano*. Bogotá, D. C., Colombia: Grupo Editorial Ibáñez.

Proaño, G. (2018). *La necesidad de incorporar al agente encubierto cibernético en la Legislación Ecuatoriana.* 22 (14), (pp. 223). Recuperado de https://www.usfq.edu.ec/publicaciones/iurisDictio/archivo_de_contenidos/Documents/IurisDictio_22/iu22_14.pdf

Silva, J. (2001). *La expansión del derecho penal: aspectos de la política criminal en las sociedad posindustriales.* Madrid, España: Civitas Ediciones S.L.

Simonetti, J. (2016). Un orden problemático. En Olaeta, Hernán, (cdd.), *Delincuencia económica organizada. Tres aproximaciones desde la criminología* (pp. 8-40). Quilmes: PGD.

Tribunal Europeo de Derechos Humanos. (26 de marzo de 1987) Sentencia No. 9248/81. [Dr. Rolv Ryssdal].

Unión Internacional de Telecomunicaciones. (2009). *El ciberdelito: Guía para los países en desarrollo*. Recuperado de EL CIBERDELITO: GUÍA PARA LOS PAÍSES EN DESARROLLO (itu.int)

Unión Internacional de Telecomunicaciones. (2022). *Measuring digital development: Facts and Figures 2022.* Recuperado de https://www.itu.int/hub/publication/d-ind-ict_mdd-2022/

Zaffaroni, E. (2008). *Globalización y crimen organizado.* Recuperado de https://www.penal.org/sites/default/files/files/Guadalajara-Zaffaroni.pdf